Enfoques de backup y recuperación en AWS

AWS Guía prescriptiva

AWS Guía prescriptiva: Enfoques de backup y recuperación en AWS

Table of Contents

Enfoques de backup y recuperación en AWS

Khurram Nizami, Amazon Web Services (AWS)

Junio de 2024 (historial de documentos)

Esta guía explica cómo implementar enfoques de respaldo y recuperación mediante los servicios de Amazon Web Services (AWS) para arquitecturas en las instalaciones, nativas en la nube e híbridas. Estos enfoques ofrecen costos más bajos, mayor escalabilidad y más durabilidad para cumplir un objetivo de tiempo de recuperación (RTO), un objetivo de punto de recuperación (RPO) y requisitos de cumplimiento.

Esta guía está destinada a los líderes técnicos responsables de proteger los datos en sus entornos corporativos de TI y de nube.

Esta guía incluye varias arquitecturas de respaldo (aplicaciones nativas en la nube, entornos híbridos y en las instalaciones). También cubre los servicios asociados de Amazon Web Services (AWS) que se pueden utilizar para crear soluciones de protección de datos escalables y fiables para los componentes no inmutables de su arquitectura.

Otro enfoque consiste en modernizar las cargas de trabajo para utilizar arquitecturas inmutables, lo que reduce la necesidad de realizar copias de seguridad y recuperación de los componentes. AWS proporciona una serie de servicios para implementar arquitecturas inmutables y reducir la necesidad de copias de seguridad y recuperación, entre los que se incluyen:

- Sin servidor con AWS Lambda
- Contenedores con Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) y AWS Fargate
- Imagen de máquina de Amazon (AMI) con Amazon Elastic Compute Cloud (Amazon EC2)

A medida que se acelera el crecimiento de los datos empresariales, la tarea de protegerlos se hace más difícil. Son frecuentes las dudas sobre la durabilidad y la escalabilidad de los enfoques de copia de seguridad, como la siguiente: ¿Cómo ayuda la nube a satisfacer mis necesidades de copia de seguridad y restauración?

Esta guía incluye los siguientes temas:

¿Por qué utilizarlos AWS como plataforma de protección de datos?

AWS es una plataforma de computación en la easy-to-use nube segura, de alto rendimiento, flexible y que ahorra dinero. AWS se ocupa del trabajo pesado e indiferenciado que se requiere para crear, implementar y administrar soluciones escalables de respaldo y recuperación.

Su uso AWS como parte de su estrategia de protección de datos tiene muchas ventajas:

- Durabilidad: Amazon Simple Storage Service (Amazon S3) y S3 Glacier Deep Archive están diseñados para ofrecer una durabilidad del 99,999999999 por ciento (11 nueves). Ambas plataformas ofrecen copias de seguridad fiables de los datos, con la replicación de objetos en al menos tres zonas de disponibilidad dispersas geográficamente. Muchos AWS servicios utilizan Amazon S3 para las operaciones de almacenamiento y exportación/importación. Por ejemplo, Amazon Elastic Block Store (Amazon EBS) utiliza Amazon S3 para el almacenamiento de instantáneas.
- Seguridad: AWS ofrece una serie de opciones para el control de acceso y el cifrado de datos tanto en tránsito como en reposo.
- Infraestructura global: AWS los servicios están disponibles en todo el mundo, por lo que puede realizar copias de seguridad de los datos y almacenarlos en la región en función de sus requisitos de cumplimiento y carga de trabajo.
- Cumplimiento: la AWS infraestructura está certificada para cumplir con los siguientes estándares, por lo que puede adaptar fácilmente la solución de respaldo a su régimen de cumplimiento actual:
  - Controles de organización de servicios (SOC)

  - Declaración sobre las normas para los contratos de certificación (SSAE) 16
  - Organización Internacional de Normalización (ISO) 27001
  - La norma de seguridad de datos del sector de pagos con tarjeta (PCI DSS)
  - Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (Health Insurance Portability and Accountability Act, HIPAA).
  - SEC1
  - Programa Federal de Administración de Riesgos y Autorizaciones (Federal Risk and Authorization Management Program, FedRAMP)
- Escalabilidad: con eso AWS, no tiene que preocuparse por la capacidad. A medida que cambien sus necesidades, puede aumentar o reducir su consumo sin gastos administrativos.
- Menor costo total de propiedad (TCO): la escala de AWS las operaciones reduce los costos de los servicios y ayuda a reducir el TCO de los servicios. AWS AWS transfiere estos ahorros de costos a los clientes mediante reducciones de precios.
- ay-as-you-go Precios P: compre AWS los servicios a medida que los necesite y solo durante el período en que planea usarlos. AWS Los precios no incluyen cargos por adelantado, multas por rescisión ni contratos a largo plazo.

Resultados empresariales específicos

El objetivo de esta guía es proporcionar información general de los servicios AWS que pueda utilizar para respaldar los enfoques de copia de seguridad y recuperación para lo siguiente:

- Arquitecturas en las instalaciones
- Arquitecturas nativas en la nube
- Arquitecturas híbridas
- Servicios nativos de AWS
- Recuperación de desastres (DR)

Se describen las prácticas recomendadas y consideraciones junto con una descripción general de los servicios. Esta guía también proporciona información sobre las compensaciones que supone utilizar un enfoque en lugar de otro para la copia de seguridad y la recuperación.

Elección AWS de servicios de protección de datos

> **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.

AWS proporciona una serie de servicios de almacenamiento y complementarios que se pueden utilizar como parte de su enfoque de copia de seguridad y recuperación. Estos servicios admiten arquitecturas híbridas y nativas en la nube. Los diferentes servicios son más eficaces para diferentes casos de uso.

- Amazon S3 es adecuado tanto para casos de uso híbridos como nativos de la nube. Proporciona soluciones de almacenamiento de objetos de uso general y muy duraderas que son adecuadas para realizar copias de seguridad de archivos individuales, servidores o un centro de datos completo.
- AWS Storage Gatewayes ideal para casos de uso híbridos. Storage Gateway utiliza la potencia de Amazon S3 para los requisitos habituales de backup y almacenamiento en las instalaciones. Sus aplicaciones se conectan al servicio a través de una máquina virtual (VM) o un dispositivo de puerta de enlace de hardware mediante los siguientes protocolos de almacenamiento estándar:
  - Sistema de archivos de red () NFS
  - Bloque de mensajes del servidor (SMB)
  - Interfaz de sistema informático pequeño de Internet (iSCSI)

  La puerta de enlace conecta estos protocolos locales comunes con servicios AWS de almacenamiento como los siguientes:
  - Amazon S3
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway facilita el suministro de almacenamiento elástico y de alto rendimiento para archivos, volúmenes, instantáneas y cintas virtuales. AWS

- AWS Backupes un servicio de respaldo totalmente administrado para centralizar y automatizar el respaldo de los datos en todos los servicios. AWS Con AWS Backup, puede configurar de forma centralizada las políticas de copias de seguridad y monitorear la actividad de copias de seguridad en busca de recursos AWS , como los siguientes:
  - EBSvolúmenes
  - EC2instancias (incluidas las aplicaciones de Windows)
  - Bases de datos de Amazon RDS y Amazon Aurora
  - Tablas de DynamoDB
  - Bases de datos de Amazon Neptune
  - Bases de datos de Amazon DocumentDB (con compatibilidad con MongoDB)
  - Sistemas de EFS archivos de Amazon
  - Sistemas de archivos Amazon FSx para Lustre y sistemas de archivos Amazon FSx para Windows File Server
  - VMwarecargas de trabajo locales y en la nube VMware AWS
  - Volúmenes de Storage Gateway

  El costo de AWS Backup se basa en el almacenamiento que consuma, restaure y transfiera en un mes. Para obtener más información, consulte los precios AWS Backup.
- AWS Elastic Disaster Recoveryreplica continuamente sus máquinas en un área de almacenamiento de bajo costo en su AWS cuenta objetivo y región preferida. Puede usar Elastic Disaster Recovery para una recuperación ante desastres y para una recuperación ante desastres entre regiones premises-to-cloud
- AWS Configproporciona una vista detallada de la configuración de AWS los recursos de su AWS cuenta. Esto incluye cómo se relacionan los recursos entre sí y cómo se han configurado en el pasado. En esta vista, puede ver cómo la configuración y las relaciones de los recursos han cambiado con el tiempo.

  Al activar el registro de la AWS Config configuración de AWS los recursos, se mantiene un historial de las relaciones entre los recursos a lo largo del tiempo. Esto ayuda a identificar y realizar un seguimiento de las relaciones entre los AWS recursos (incluidos los recursos eliminados) durante un máximo de siete años. Por ejemplo, AWS Config puede rastrear la relación entre un volumen de EBS instantáneas de Amazon y la EC2 instancia a la que se adjuntó el volumen.
- AWS Lambdase puede utilizar para definir y automatizar mediante programación los procedimientos de respaldo y recuperación de sus cargas de trabajo. Puede usarlo AWS SDKs

para interactuar con AWS los servicios y sus datos. También puede usar Amazon CloudWatch Events para ejecutar las funciones de Lambda de forma programada.

AWS los servicios proporcionan funciones específicas para la copia de seguridad y la restauración. Para cada AWS servicio que utilice, consulte la AWS documentación para determinar las funciones de copia de seguridad, restauración y protección de datos que ofrece el servicio. Puede usar AWS Command Line Interface (AWS CLI) y las API operaciones para automatizar las funciones AWS específicas del servicio para la copia de seguridad y la recuperación de datos. AWS SDKs

Diseño de una solución de respaldo y recuperación

Al desarrollar una estrategia integral para realizar copias de seguridad y restaurar datos, primero debe identificar las posibles situaciones de fallo o desastre y su posible impacto en el negocio. En algunos sectores, debe tener en cuenta los requisitos reglamentarios en materia de seguridad de los datos, privacidad y conservación de registros.

Los procesos de backup y recuperación deben incluir el nivel de granularidad adecuado para cumplir con el objetivo de tiempo de recuperación (RTO) y el objetivo de punto de recuperación (RPO) para la carga de trabajo y sus procesos empresariales de apoyo, incluidos los siguientes:

- Recuperación a nivel de archivos (por ejemplo, archivos de configuración de una aplicación)
- Recuperación a nivel de datos de la aplicación (por ejemplo, una base de datos específica dentro de MySQL)
- Recuperación a nivel de aplicación (por ejemplo, una versión específica de una aplicación de servidor web)
- Recuperación a nivel de volumen de Amazon EC2 (por ejemplo, un volumen de EBS)
- Recuperación a nivel de instancia de EC2. (por ejemplo, una instancia EC2)
- Recuperación de servicios gestionados (por ejemplo, una tabla de DynamoDB)

Asegúrese de tener en cuenta todos los requisitos de recuperación de la solución y las dependencias de datos entre los distintos componentes de la arquitectura. Para facilitar un proceso de restauración exitoso, coordine el respaldo y la recuperación entre los distintos componentes de su arquitectura.

En los siguientes temas se describen los enfoques de respaldo y recuperación en función de la organización de la infraestructura. En términos generales, la infraestructura de TI se puede clasificar como en las instalaciones, híbrida o nativa en la nube.

Copia de seguridad y recuperación mediante AWS Backup

AWS Backup es un servicio de copia de seguridad completamente administrado que centraliza y automatiza las copias de seguridad de datos en servicios AWS. AWS Backup proporciona una capa de orquestación que integra Amazon CloudWatch, AWS CloudTrail, AWS Identity and Access Management (IAM), AWS Organizations y otros servicios. Esta solución centralizada y nativa en la nube AWS ofrece capacidades de copias de seguridad globales que pueden ayudarle a cumplir sus requisitos de conformidad y recuperación de desastres. Con AWS Backup, puede configurar de forma centralizada las políticas de copias de seguridad y monitorear la actividad de copias de seguridad en busca de recursos AWS.

AWS Backup es una solución ideal para implementar planes de copias de seguridad estándar para sus recursos AWS en todas sus cuentas AWS y regiones. Como AWS Backup admite varios tipos de recursos AWS, facilita el mantenimiento y la implementación de una estrategia de copias de seguridad para las cargas de trabajo que utilizan varios recursos AWS de los que es necesario realizar copias de seguridad de forma colectiva. AWS Backup también le permite supervisar de forma colectiva una operación de copia de seguridad y restauración que implica varios recursos AWS.

Si tiene requisitos de conformidad y auditoría, puede utilizar la característica AWS BackupAudit Manager para crear marcos e informes de auditoría que respalden sus requisitos de conformidad. La característica AWS BackupVault Lock también cumple con los requisitos de conformidad al aplicar una configuración de escritura única y lectura múltiple (WORM) para todas las copias de seguridad almacenadas en una bóveda de copias de seguridad. AWS Backup

Un elemento diferenciador clave de AWS Backup es el apoyo a las organizaciones. Con este soporte, puede definir y administrar las políticas de copias de seguridad a nivel de la organización o unidad organizativa, y hacer que esas políticas se implementen automáticamente para cada cuenta AWS y región relacionadas. A medida que incorpore nuevas cuentas AWS y regiones, no tendrá que definir ni administrar los planes de copias de seguridad por separado.

AWS Backup puede facilitar la implementación de una política de copias de seguridad para toda la organización mediante el uso de etiquetas. Puede crear planes de copia de seguridad independientes que tengan cada uno una configuración de frecuencia y retención única y, a continuación, crear etiquetas de par clave-valor únicas que seleccionen los recursos que se incluirán en la copia de seguridad.

Por ejemplo, puede crear un plan de copia de seguridad diario que inicie una copia de seguridad a las 05:00 UTC todos los días y que tenga una política de retención de 35 días. Este plan de

copia de seguridad puede incluir una asignación de recursos de copia de seguridad en la que se especifique que se realizará una copia de seguridad de todos los recursos AWScompatibles con la copia de seguridad de la clave de etiqueta y el valor de la etiqueta a diario, de acuerdo con este plan. Además, puede crear un plan de copias de seguridad mensual que comience a las 05:00 UTC del primer día de cada mes y que tenga una política de retención de 366 días. Este plan de copias de seguridad puede incluir una asignación de recursos de copias de seguridad que especifique que cualquier recurso AWS compatible con la copia de seguridad de la clave de etiqueta y el valor de la etiqueta se incluirá mensualmente en la copia de seguridad, de acuerdo con este plan.

A continuación, puede utilizar las políticas de etiquetas y la regla AWS Config de etiquetas obligatorias para asegurarse de que todos los recursos AWS compatibles tengan esta clave de etiqueta y uno de estos valores de etiqueta. Este enfoque puede ayudarlo a implementar y mantener de manera consistente un enfoque de copias de seguridad estándar AWS para los recursos compatibles AWS Backup. Puede ampliar este enfoque para estandarizar los copias de seguridad de sus aplicaciones y capas de arquitectura que tienen diferentes requisitos de objetivo de punto de recuperación (RPO).

Le recomendamos que tome medidas para proteger su almacén de copias de seguridad. Por ejemplo, puede implementar una política de control de servicios (SCP) de una organización que impida que su almacén de copias de seguridad se elimine o se comparta con cuentas AWS no deseadas. Para obtener más información y otras consideraciones de seguridad importantes, consulte las 10 mejores prácticas de seguridad para proteger las copias de seguridad en AWS una entrada de blog.

AWS Backup puede simplificar la implementación de su plan de recuperación de desastres (DR) para AWS, porque admite varios recursos AWS que pueden abordarse de forma colectiva. Por ejemplo, puede implementar copias de seguridad entre regiones y entre cuentas para la mayoría de los tipos de recursos AWS compatibles con AWS Backup. La copia de seguridad multicuenta mejora la seguridad de la copia de seguridad, ya que hay una copia disponible en una cuenta independiente. Las copias de seguridad entre regiones mejoran la disponibilidad porque las copias de seguridad están disponibles en más de una región. Para obtener más información sobre los tipos de recursos AWS compatibles, consulte la tabla Disponibilidad de características por recurso.

Puede usar el ejemplo de solución de código abierto para copias de seguridad y recuperación con AWS Backup para implementar un enfoque de infraestructura como código (IaC), así como la integración y entrega continua (CI/CD) para administrar los copias de seguridad de su organización. AWS Organizations Esta solución incluye características personalizadas, como volver a aplicar automáticamente etiquetas AWS en los recursos restaurados AWS y establecer un almacén de

copias de seguridad secundario en una cuenta y región independientes para fines de recuperación de desastres.

Backup y recuperación mediante Amazon S3

Puede utilizar Amazon Simple Storage Service (Amazon S3) para almacenar y recuperar cualquier cantidad de datos en cualquier momento. Puede utilizar Amazon S3 como almacén duradero para los datos de sus aplicaciones y los procesos de copia de seguridad y restauración a nivel de archivo. Por ejemplo, puede copiar las copias de seguridad de su base de datos desde una instancia de base de datos a Amazon S3 con un script de copia de seguridad mediante los AWS SDK AWS CLI o los SDK.

Servicios de AWS utilice Amazon S3 para un almacenamiento fiable y de alta durabilidad, como en los ejemplos siguientes:

- Amazon EC2 utiliza Amazon S3 para almacenar instantáneas de Amazon EBS para volúmenes de EBS y para almacenes de instancias EC2.
- Storage Gateway se integra con Amazon S3 para proporcionar entornos locales con bibliotecas de cintas, volúmenes y recursos compartidos de archivos respaldados por Amazon S3.
- Amazon RDS utiliza Amazon S3 para instantáneas de base de datos.

Muchas soluciones de copia de seguridad de terceros también utilizan Amazon S3. Por ejemplo, Arcserve Unified Data Protection es compatible con Amazon S3 para realizar copias de seguridad duraderas de servidores en las instalaciones y nativos en la nube.

Puede utilizar las funciones integradas de Amazon S3 de estos servicios para simplificar su enfoque de backup y recuperación. Al mismo tiempo, puede beneficiarse de la alta durabilidad y disponibilidad que ofrece Amazon S3.

Amazon S3 almacena datos como objetos dentro de recursos denominados buckets. Puede almacenar la cantidad de objetos que desee en un bucket. Puede escribir, leer y eliminar objetos de su bucket con un control de acceso detallado. Los objetos individuales pueden tener un tamaño máximo de 5 TB.

Uso de las clases de almacenamiento de Amazon S3 para reducir los costos de almacenamiento de datos de respaldo

Amazon S3 ofrece varias clases de almacenamiento para su uso en arquitecturas locales, híbridas y nativas de la nube. Todas las clases de almacenamiento proporcionan una capacidad escalable que no requiere la administración de volúmenes o medios a medida que crecen sus conjuntos de datos

de respaldo. El modelo pay-for-what-you de uso y el bajo costo por GB al mes hacen que las clases de almacenamiento de Amazon S3 sean adecuadas para una amplia gama de casos de uso de protección de datos. Las clases de almacenamiento de Amazon S3 están diseñadas para diferentes casos de uso, incluidas las siguientes categorías:

- Clases de almacenamiento de acceso frecuente para el almacenamiento con fines generales de los datos a los que se accede con frecuencia (por ejemplo, archivos de configuración, copias de seguridad no planificadas o copias de seguridad diarias). Esto incluye la clase de almacenamiento S3 Standard, que es la predeterminada para todos los objetos de Amazon S3.
- Clases de almacenamiento de acceso poco frecuente para datos de larga duración, pero a los que se accede con poca frecuencia (por ejemplo, copias de seguridad mensuales). Esto incluye la clase de almacenamiento S3 Standard-IA. IA significa acceso poco frecuente (infrequent access).
- Clases de almacenamiento de S3 Glacier para datos de larga duración a los que rara vez es necesario acceder (por ejemplo, copias de seguridad anuales). Esto incluye S3 Glacier Deep Archive, que proporciona el almacenamiento más económico en. AWS

Para copias de seguridad con patrones de acceso desconocidos o cambiantes, puede utilizar la clase de almacenamiento S3 Intelligent-Tiering. S3 Intelligent-Tiering transfiere automáticamente los objetos al nivel más rentable en función del tiempo transcurrido desde la última vez que se accedió a un objeto.

> **Note**
>
> Algunas clases de almacenamiento tienen un cargo por duración mínima. Para obtener más información, consulte los precios de Amazon S3 y utilice la búsqueda en la página web para encontrarlos`duration`.

Amazon S3 ofrece políticas de ciclo de vida que puede configurar para administrar sus datos a lo largo de su ciclo de vida. Una vez establecida una política, sus datos se migrarán automáticamente a la clase de almacenamiento adecuada sin que se produzca ningún cambio en la aplicación. Para obtener más información, consulte la documentación sobre la administración del ciclo de vida de los objetos de Amazon S3.

Para reducir los costos de la copia de seguridad, utilice un enfoque de clase de almacenamiento por niveles basado en el Objetivo de tiempo de recuperación (RTO) y el Objetivo de punto de recuperación (RPO), como en el siguiente ejemplo:

- Copias de seguridad diarias de las últimas 2 semanas con S3 Standard
- Copias de seguridad semanales de los últimos 3 meses con S3 Standard-IA
- Copias de seguridad trimestrales del año pasado en S3 Glacier Flexible Retrieval
- Copias de seguridad anuales de los últimos 5 años en S3 Glacier Deep Archive
- Copias de seguridad eliminadas del S3 Glacier Deep Archive después de cinco años

Creación de depósitos S3 estándar para realizar copias de seguridad y archivar

Puede crear un bucket S3 estándar para realizar copias de seguridad y archivar con la política de copias de seguridad y retención de su empresa implementada mediante las políticas de ciclo de vida de S3. La asignación de costos, el etiquetado y los informes para la AWS facturación se basan en las etiquetas asignadas a nivel de segmento. Si la asignación de costos es importante, cree buckets S3 de copia de seguridad y archivado independientes para cada proyecto o unidad de negocio, de modo que pueda asignar los costos en consecuencia.

Sus scripts y aplicaciones de respaldo pueden usar el depósito S3 de respaldo y archivado que usted cree para almacenar point-in-time instantáneas de los datos de aplicaciones y cargas de trabajo. Puede crear un prefijo S3 estándar que le ayude a organizar las instantáneas de point-in-time datos. Por ejemplo, si crea copias de seguridad cada hora, considere la posibilidad de utilizar un prefijo de copia de seguridad como `YYYY/MM/DD/HH/<WorkloadName>/<files...>`. De este modo, puede recuperar rápidamente sus point-in-time copias de seguridad de forma manual o programática.

Uso del control de versiones de Amazon S3 para mantener automáticamente el historial de reversiones

Puede activar el control de versiones de los objetos de S3 para mantener un historial de cambios en los objetos, incluida la posibilidad de volver a una versión anterior. Esto resulta útil para los archivos de configuración y otros objetos que pueden cambiar con más frecuencia que la programación de las point-in-time copias de seguridad. También es útil para los archivos que deben revertirse de forma individual.

Uso de Amazon S3 para realizar copias de seguridad y recuperar archivos de configuración personalizados para las AMI

Amazon S3 con control de versiones de objetos puede convertirse en su sistema de registro para los archivos de opciones y configuración de sus cargas de trabajo. Por ejemplo, puede utilizar una imagen estándar de AWS Marketplace Amazon EC2 mantenida por un ISV. Esta imagen puede contener software cuya configuración se mantiene en varios archivos de configuración. Puede mantener los archivos de configuración personalizados en Amazon S3. Cuando se lance la instancia, puede copiar estos archivos de configuración en la instancia como parte de los datos de usuario de la instancia. Al aplicar este enfoque, no es necesario personalizar ni volver a crear una AMI para usar una versión actualizada.

Uso de Amazon S3 en su proceso personalizado de copia de seguridad y restauración

Amazon S3 proporciona un almacén de copias de seguridad de uso general que puede integrar rápidamente en sus procesos de copias de seguridad personalizadas existentes. Puede utilizar las AWS CLI operaciones de API y AWS los SDK para integrar los scripts y procesos de backup y restauración que utilizan Amazon S3. Por ejemplo, puede tener un script de copia de seguridad de base de datos que realice exportaciones nocturnas de bases de datos. Puede personalizar este script para copiar sus copias de seguridad nocturnas a Amazon S3 para almacenarlas fuera de las instalaciones. Consulta el tutorial sobre cómo subir archivos por lotes a la nube para obtener información general sobre cómo hacerlo.

Puede adoptar un enfoque similar para exportar y hacer copias de seguridad de los datos de diferentes aplicaciones en función de su RPO individual. Además, puede utilizarlos AWS Systems Manager para ejecutar sus scripts de respaldo en sus instancias administradas. Systems Manager proporciona automatización, control de acceso, programación, registro y notificación para sus procesos de copias de seguridad individuales.

Protección de los datos de respaldo en Amazon S3

La seguridad de los datos es una preocupación universal y AWS se toma la seguridad muy en serio. La seguridad es la base de todo Servicio de AWS. Amazon S3 ofrece funciones de control de acceso y cifrado tanto en reposo como en tránsito. Todos los puntos de enlace de Amazon S3 admiten

SSL/TLS para cifrar los datos en tránsito. Puede configurar el cifrado de los objetos en reposo de la siguiente manera:

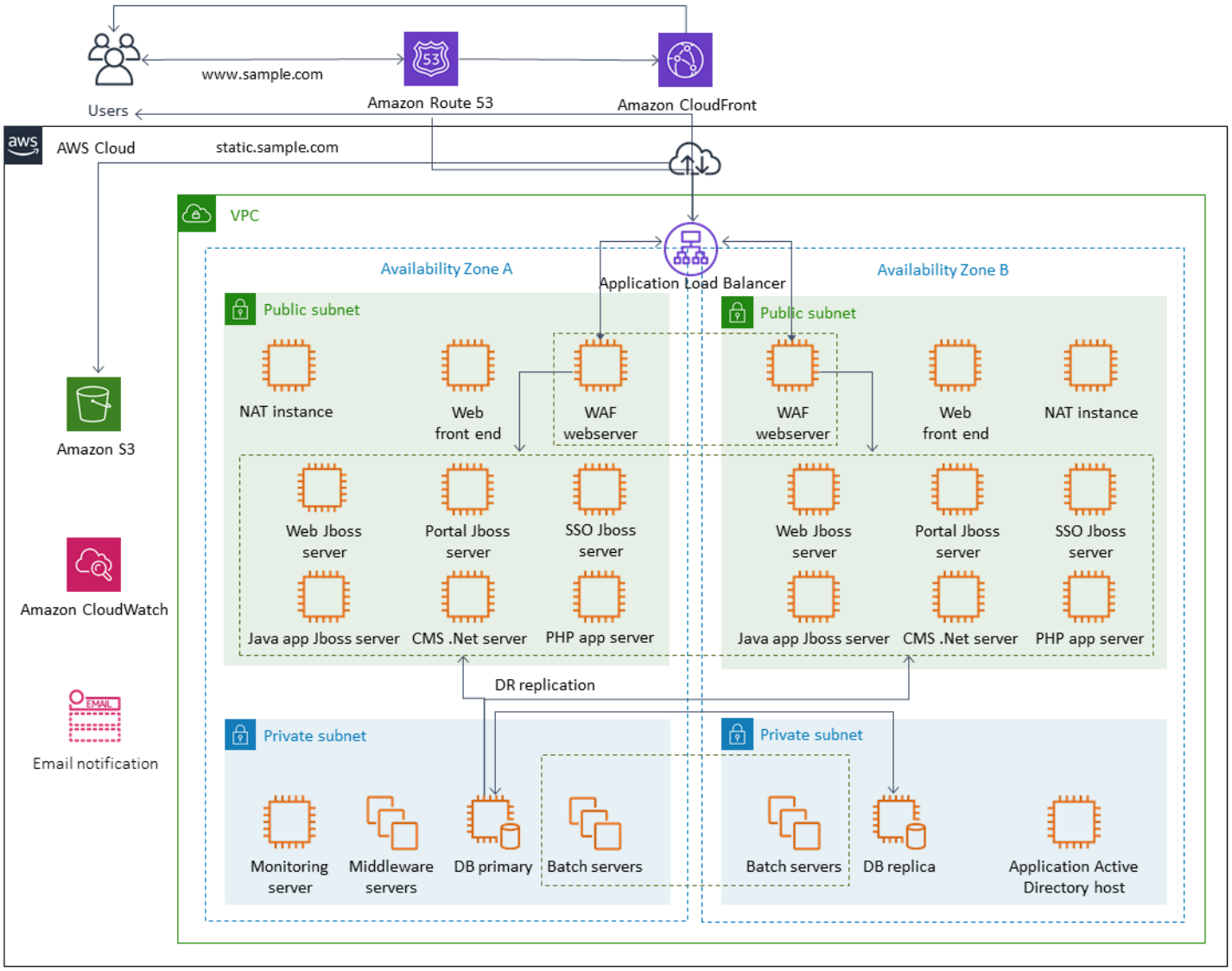
- Uso del cifrado del lado del servidor con claves de cifrado gestionadas por Amazon S3 (predeterminado)
- Uso del cifrado del lado del servidor con claves AWS Key Management Service () almacenadas AWS KMS en AWS KMS
- Uso del cifrado del lado del cliente

Puede usar AWS Identity and Access Management (IAM) para controlar el acceso a los objetos de S3. La IAM permite controlar los permisos de los objetos individuales y las rutas de prefijo específicas dentro de un bucket de S3. Puede auditar el acceso a los objetos de S3 mediante el registro a nivel de objeto con. AWS CloudTrail

Copia de seguridad y recuperación para Amazon EC2 con volúmenes de EBS

AWS proporciona varios métodos para realizar copias de seguridad de las instancias de Amazon EC2. En esta sección, se tratan distintos aspectos de la creación de copias de seguridad de volúmenes de Amazon Elastic Block Store (Amazon EBS) o de volúmenes de almacén de instancias para el almacenamiento. AWS Backup Considérelo como su primera opción para administrar las copias de seguridad AWS si cumple con sus requisitos. Recuerde que las copias de seguridad son buenas solo si se pueden restaurar para que devuelvan la función para la que fueron diseñadas. La función de restauración y recuperación debe probarse periódicamente para confirmarlo.

La arquitectura de la solución del siguiente diagrama describe un entorno de carga de trabajo que existe completamente en AWS la mayoría de las arquitecturas basadas en Amazon EC2. Como se muestra en la siguiente figura, el escenario incluye servidores web, servidores de aplicaciones, servidores de monitoreo, bases de datos y Active Directory.



AWS proporciona muchos servicios con todas las funciones para muchos de los servidores Amazon EC2 representados en esta arquitectura para realizar el trabajo indiferenciado de crear, aprovisionar, realizar copias de seguridad, restaurar y optimizar las instancias y el almacenamiento. Considere si estos servicios tienen sentido en su arquitectura para reducir la complejidad y la administración. AWS también proporciona servicios para mejorar la disponibilidad de sus arquitecturas basadas en Amazon EC2. Concretamente, tenga en cuenta Amazon EC2 Auto Scaling y Elastic Load Balancing para complementar sus cargas de trabajo en Amazon EC2. El uso de estos servicios puede mejorar la disponibilidad y la tolerancia a errores de su arquitectura y ayudarle a restaurar las instancias dañadas con un impacto mínimo para los usuarios.

Las instancias de EC2 utilizan principalmente volúmenes de Amazon EBS para el almacenamiento persistente. Amazon EBS proporciona una serie de características de copia de seguridad y recuperación que se describen en detalle en esta sección.

Temas

Copias de seguridad y recuperación de Amazon EC2 con instantáneas y AMI

Considere si necesita crear una copia de seguridad completa de una instancia EC2 con una imagen de máquina de Amazon (AMI) o tome una instantánea de un volumen individual.

Usar AMI o instantáneas de Amazon EBS para las copias de seguridad

Una AMI incluye lo siguiente:

- Una o más instantáneas. Las nstance-store-backed AMI I incluyen una plantilla para el volumen raíz de la instancia (por ejemplo, un sistema operativo, un servidor de aplicaciones y aplicaciones).
- Permisos de lanzamiento que controlan qué AWS cuentas pueden usar la AMI para lanzar instancias.
- Una asignación de dispositivos de bloques que especifica los volúmenes que se van a adjuntar a la instancia cuando se lance.

Puede usar las AMI para lanzar nuevas instancias con software y datos preconfigurados. Puede crear AMI cuando desee establecer una línea base, que es una configuración reutilizable para lanzar más instancias. Cuando se crea una AMI de una instancia de EC2 existente, se crea una instantánea de todos los volúmenes que están asociados a la instancia. La instantánea incluye las asignaciones de dispositivos.

No se pueden utilizar instantáneas para lanzar una nueva instancia, pero se pueden usar para reemplazar los volúmenes de una instancia existente. Si los datos están dañados o se produce un error en el volumen, puede crear un volumen a partir de una instantánea que haya tomado

y reemplazar el volumen anterior. También puede usar instantáneas para aprovisionar nuevos volúmenes y adjuntarlos durante el lanzamiento de una nueva instancia.

Si utiliza AMI de plataforma y aplicación mantenidas y publicadas por AWS o desde la AWS Marketplace, considere la posibilidad de mantener volúmenes separados para sus datos. Puede hacer copias de seguridad de los volúmenes de datos como instantáneas independientes de los volúmenes del sistema operativo y de las aplicaciones. A continuación, utilice las instantáneas del volumen de datos con las AMI recién actualizadas publicadas por AWS o desde. AWS Marketplace Este enfoque requiere pruebas y una planificación cuidadosas para realizar copias de seguridad y restaurar todos los datos personalizados, incluida la información de configuración, en las AMI recién publicadas.

El proceso de restauración se ve afectado por la elección entre copias de seguridad de las AMI o de las instantáneas. Si crea AMI para que sirvan como copias de seguridad de instancias, debe lanzar una instancia EC2 desde la AMI como parte del proceso de restauración. Es posible que también deba cerrar la instancia existente para evitar posibles colisiones. Un ejemplo de posible colisión son los identificadores de seguridad (SID) de las instancias de Windows unidas a un dominio. El proceso de restauración de las instantáneas puede requerir que separe el volumen existente y adjunte el volumen recién restaurado. O puede que necesite realizar un cambio de configuración para dirigir las aplicaciones al volumen recién conectado.

AWS Backup admite copias de seguridad a nivel de instancia como AMI y copias de seguridad a nivel de volumen como instantáneas independientes:

- Para realizar una copia de seguridad completa de todos los volúmenes de EBS de la instancia, cree una AMI de la instancia EC2 que se ejecuta en Linux o Windows. Cuando desee revertirla, utilice el asistente de lanzamiento de instancias para crear una instancia. En el asistente de lanzamiento de instancias, selecciona Mis AMI.
- Para hacer una copia de seguridad de un volumen individual, cree una instantánea. Para restaurar la instantánea, consulte Crear un volumen a partir de una instantánea. Puede usar el AWS Management Console o el AWS Command Line Interface (AWS CLI).

El costo de una AMI de instancia es el almacenamiento de todos los volúmenes de la instancia, pero no de los metadatos. El costo de una instantánea de EBS es el almacenamiento del volumen individual. Para obtener más información sobre los costes de almacenamiento por volumen, consulte la página de precios de Amazon EBS.

Volúmenes de servidores

Los volúmenes de EBS son la principal opción de almacenamiento persistente para Amazon EC2. Puede utilizar este almacenamiento en bloques para datos estructurados, como bases de datos, o datos no estructurados, como los archivos de un sistema de archivos de un volumen.

Los volúmenes de EBS se encuentran en una zona de disponibilidad específica. Los volúmenes se replican en varios servidores para evitar la pérdida de datos por el fallo de un solo componente. El fallo se refiere a una pérdida total o parcial del volumen, según el tamaño y el rendimiento del volumen.

Los volúmenes de EBS están diseñados para una tasa de error anual (AFR) del 0,1 al 0,2 por ciento. Esto hace que los volúmenes de EBS sean 20 veces más de confianza que las unidades de disco habituales, que fallan con un AFR de alrededor del 4 por ciento. Por ejemplo, si tiene 1000 volúmenes de EBS en funcionamiento durante un año, cabe esperar que se produzcan errores en uno o dos volúmenes.

Amazon EBS también admite una función de instantáneas para realizar point-in-time copias de seguridad de sus datos. Todos los tipos de volumen de EBS ofrecen funcionalidad de instantáneas y están diseñados para tener una disponibilidad del 99,999 %. Para obtener más información, consulte el Acuerdo de nivel de servicios de Amazon Compute.

Amazon EBS ofrece la posibilidad de crear instantáneas (copias de seguridad) de cualquier volumen de EBS. Una instantánea es una característica básica para crear copias de seguridad de sus volúmenes de EBS. Una instantánea toma una copia del volumen de EBS y la coloca en Amazon S3, donde se almacena de forma redundante en varias zonas de disponibilidad. La instantánea inicial es una copia completa del volumen; las instantáneas continuas solo almacenan los cambios incrementales a nivel de bloque. Consulte la documentación de Amazon EC2 para obtener detalles sobre cómo crear instantáneas de Amazon EBS.

Puede realizar una operación de restauración, eliminar una instantánea o actualizar los metadatos de la instantánea, como las etiquetas, asociados a la instantánea desde la consola Amazon EC2 en la misma región en la que realizó la instantánea.

Al restaurar una instantánea, se crea un nuevo volumen de Amazon EBS con los datos del volumen completo. Si solo necesita una restauración parcial, puede adjuntar el volumen a la instancia en ejecución con un nombre de dispositivo diferente. A continuación, móntelo y utilice los comandos de copia del sistema operativo para copiar los datos del volumen de copias de seguridad al volumen de producción.

Las instantáneas de Amazon EBS también se pueden copiar entre AWS regiones mediante la capacidad de copia de instantáneas de Amazon EBS, tal y como se describe en la documentación de Amazon EC2. Puede utilizar esta característica para almacenar la copia de seguridad en otra región sin tener que gestionar la tecnología de replicación subyacente.

Establecer volúmenes de servidores separados

Es posible que ya utilice un conjunto estándar de volúmenes independientes para el sistema operativo, los registros, las aplicaciones y los datos. Al establecer volúmenes de servidor separados, puede reducir el alcance del impacto en caso de que se produzcan errores en las aplicaciones o plataformas debido al agotamiento del espacio en disco. Este riesgo suele ser mayor con los discos duros físicos, ya que no se cuenta con la flexibilidad necesaria para ampliar los volúmenes rápidamente. En el caso de las unidades físicas, debe adquirir las nuevas unidades, realizar copias de seguridad de los datos y, a continuación, restaurarlos en las nuevas unidades. Con ello AWS, este riesgo se reduce considerablemente, ya que puede utilizar Amazon EBS para ampliar los volúmenes aprovisionados. Para obtener más información, consulte la Documentación de AWS.

Mantenga volúmenes separados para los datos de las aplicaciones, los datos de los usuarios, los registros y los archivos de intercambio, de modo que pueda utilizar políticas de copia de seguridad y restauración independientes para estos recursos. Al separar los volúmenes de sus datos, también puede usar diferentes tipos de volúmenes en función de los requisitos de rendimiento y almacenamiento de los datos. A continuación, puede optimizar y ajustar los costos para las diferentes cargas de trabajo.

Consideraciones, por ejemplo, volúmenes de almacenes de instancias

El almacén de instancias ofrece un almacenamiento por bloques temporal para la instancia. Este almacenamiento se encuentra en discos que están conectados físicamente al equipo host. Los almacenes de instancias son ideales para el almacenamiento temporal de información que cambia constantemente, como los búferes, las cachés, los datos de pruebas y otro contenido temporal. También son preferibles para los datos que se replican en una flota de instancias, como un grupo de servidores web con equilibrio de carga.

Los datos en cualquier almacén de instancias se conservan solo durante el ciclo de vida de la instancia asociada. Si una instancia se reinicia (de manera intencionada o no intencionada), los datos del almacén de instancias se conservan. Sin embargo, los datos del almacén de instancias se pierden en cualquiera de las siguientes circunstancias.

- Falla la unidad de disco subyacente.

- Si se detiene la instancia.
- Si la instancia termina.

Por lo tanto, no confíe en el almacén de instancias para almacenar datos valiosos a largo plazo. En su lugar, utilice un almacenamiento de datos más duradero, como Amazon S3, Amazon EBS o Amazon EFS.

Una estrategia habitual con los volúmenes de almacenes de instancias consiste en conservar los datos necesarios en Amazon S3 con regularidad según sea necesario, en función del objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO). A continuación, puede descargar los datos de Amazon S3 a su almacén de instancias cuando se lance una nueva instancia. También puede cargar los datos en Amazon S3 antes de detener una instancia. Para mantener la persistencia, cree un volumen de EBS, adjúntelo a su instancia y copie los datos del volumen del almacén de instancias al volumen de EBS de forma periódica. Para obtener más información, consulte el Centro de conocimientos de AWS.

Etiquetar y aplicar los estándares para las instantáneas y las AMI de EBS

Etiquetar todos sus AWS recursos es una práctica importante para la asignación de costos, la auditoría, la solución de problemas y la notificación. El etiquetado es importante para los volúmenes de EBS, de modo que esté presente la información pertinente necesaria para administrar y restaurar los volúmenes. Las etiquetas no se copian automáticamente de las instancias EC2 a las AMI ni de los volúmenes de origen a las instantáneas. Asegúrese de que el proceso de copia de seguridad incluya las etiquetas pertinentes de estas fuentes. Esta opción sirve de ayuda para configurar los metadatos de las instantáneas, como las políticas de acceso, la información de datos adjuntos y la asignación de costos, para utilizar estas copias de seguridad en el futuro. Para obtener más información sobre cómo etiquetar sus AWS recursos, consulte el documento técnico sobre las mejores prácticas de etiquetado.

Además de las etiquetas que utilice para todos los AWS recursos, utilice las siguientes etiquetas específicas para las copias de seguridad:

- ID de instancia de origen
- ID del volumen de origen (para instantáneas)
- Descripción del punto de recuperación

Puede aplicar las políticas de etiquetado mediante AWS Config reglas y permisos de IAM. IAM admite el uso obligatorio de etiquetas, por lo que puede redactar políticas de IAM que exijan el uso de etiquetas específicas al actuar sobre las instantáneas de Amazon EBS. Si se intenta realizar una `CreateSnapshot` operación sin que las etiquetas definidas en la política de permisos de IAM concedan derechos, se produce un error en la creación de la instantánea y se deniega el acceso. Para obtener más información, consulte la entrada del blog sobre el etiquetado de las instantáneas de Amazon EBS al crear e implementar políticas de seguridad más sólidas.

Puede usar AWS Config reglas para evaluar automáticamente los ajustes de configuración de sus AWS recursos. Para ayudarle a empezar, AWS Config proporciona reglas personalizables y predefinidas denominadas reglas administradas. También puede crear sus propias reglas personalizadas. Si bien realiza un seguimiento AWS Config continuo de los cambios de configuración de sus recursos, comprueba si estos cambios infringen alguna de las condiciones de las reglas. Si un recurso infringe una regla, AWS Config marca el recurso y la regla como no conformes. Tenga en cuenta que la regla de administración de etiquetas obligatorias actualmente no admite instantáneas ni AMI.

Creación de copias de seguridad de volúmenes de EBS con AMI e instantáneas de EBS

AWS ofrece una amplia variedad de opciones para crear y administrar AMI e instantáneas. Puede utilizar el enfoque que se ajuste a sus necesidades. Un problema común al que se enfrentan muchos clientes es administrar el ciclo de vida de las instantáneas y alinearlas claramente según el propósito, la política de retención, etc. Sin el etiquetado adecuado, existe el riesgo de que las instantáneas se eliminen accidentalmente o como parte de un proceso de limpieza automatizado. También es posible que acabe pagando por las instantáneas obsoletas que se conservan, porque no se sabe con claridad si siguen siendo necesarias.

Preparación de un volumen de EBS antes de crear una instantánea o una AMI

Antes de tomar una instantánea o crear una AMI, realice los preparativos necesarios para el volumen de EBS. La creación de una AMI da como resultado una nueva instantánea para cada volumen de EBS adjunto a la instancia, por lo que estos preparativos también se aplican a las AMI.

Puede tomar una instantánea de un volumen EBS adjunto que esté siendo utilizado por una instancia EC2 encendida. Sin embargo, las instantáneas solo capturan los datos que se han escrito en el

volumen de su EBS en el momento que se lanza el comando snapshot. Esto puede excluir los datos que las aplicaciones o el sistema operativo hayan guardado en la memoria caché. La mejor práctica es tener el sistema en un estado en el que no se realicen operaciones de E/S. Lo ideal es que la máquina no acepte tráfico y se encuentre parada, pero esto es poco frecuente, ya que las operaciones de TI ininterrumpidas se han convertido en la norma. Si puede vaciar cualquier dato de la memoria del sistema en el disco utilizado por las aplicaciones y detener la escritura de archivos en el volumen el tiempo suficiente para realizar una instantánea, la instantánea debería estar completa.

Para realizar una copia de seguridad limpia, debe poner en reposo la base de datos o el sistema de archivos. La forma de hacerlo depende de la base de datos o del sistema de archivos.

El proceso para crear una base de datos de es el siguiente:

1. Si es posible, ponga la base de datos en modo de copia de seguridad activa.
2. Ejecute los comandos de instantáneas de Amazon EBS.
3. Saque la base de datos del modo de copia de seguridad activa o, si utiliza una réplica de lectura, finalice la instancia de réplica de lectura.

El proceso de un sistema de archivos es similar, pero depende de las capacidades del sistema operativo o del sistema de archivos. Por ejemplo, XFS es un sistema de archivos que puede vaciar sus datos para obtener una copia de seguridad coherente. Para obtener más información, consulte xfs_freeze. Como alternativa, puede facilitar este proceso mediante el uso de un administrador de volúmenes lógico que permita congelar las E/S.

Sin embargo, si no puede vaciar o pausar todas las escrituras de archivos en el volumen, haga lo siguiente:

1. Desconectar el volumen del sistema operativo.
2. Ejecute el comando de instantánea.
3. Vuelva a montar el volumen para obtener una instantánea completa y coherente. Puede volver a montar y usar el volumen mientras el estado de la instantánea esté pendiente.

El proceso de la instantánea continúa en segundo plano y la creación de instantáneas es rápida y captura un punto en el tiempo. Los volúmenes de los que está haciendo copias de seguridad se desmontan solo en cuestión de segundos. Puede programar una pequeña ventana de copia de seguridad en la que se espere que se produzca una interrupción y los clientes la gestionen sin problemas.

Al crear una instantánea para un volumen de EBS que actúa como dispositivo raíz, debe parar la instancia antes de tomar la instantánea. Windows proporciona el servicio Volume Shadow Copy (VSS) para ayudar a crear instantáneas coherentes con las aplicaciones. AWS proporciona un documento de Systems Manager que puede ejecutar para realizar copias de seguridad a nivel de imagen de aplicaciones compatibles con VSS. Las instantáneas incluyen datos de transacciones pendientes entre estas aplicaciones y el disco. No es necesario que apague sus instancias o las desconecte cuando respalde todos los volúmenes adjuntos. Para obtener más información, consulte la Documentación de AWS.

> **Note**
>
> Si va a crear una AMI de Windows para poder implementar otra instancia similar, utilice EC2Config o EC2Launch para Sysprep su instancia. Cree una AMI a partir de la instancia detenida. Sysprep elimina información exclusiva de la instancia Amazon EC2 de Windows, incluidos los SID, el nombre del equipo y los controladores. Los SID duplicados pueden provocar problemas con Active Directory, Windows Server Update Services (WSUS), problemas de inicio de sesión, activación de claves de volumen de Windows, Microsoft Office y productos de terceros. No utilice Sysprep con la instancia si la AMI sirve para realizar copias de seguridad y desea restaurar la misma instancia con toda su información exclusiva intacta.

Creación manual de instantáneas de volúmenes de EBS desde la consola

Cree instantáneas de los volúmenes correspondientes o de toda la instancia antes de realizar cambios importantes que no se hayan probado completamente en la instancia. Por ejemplo, es posible que quiera crear una instantánea antes de actualizar o parchear el software de la aplicación o del sistema de la instancia.

Puede crear una instantánea de forma manual desde la consola. En la consola de Amazon EC2, en la página Volúmenes de Elastic Block Store, seleccione el volumen del que quiere hacer una copia de seguridad. En el menú Acciones, elija Crear instantánea. Para buscar los volúmenes adjuntos a una instancia específica, introduzca el ID de la instancia en el cuadro de filtro.

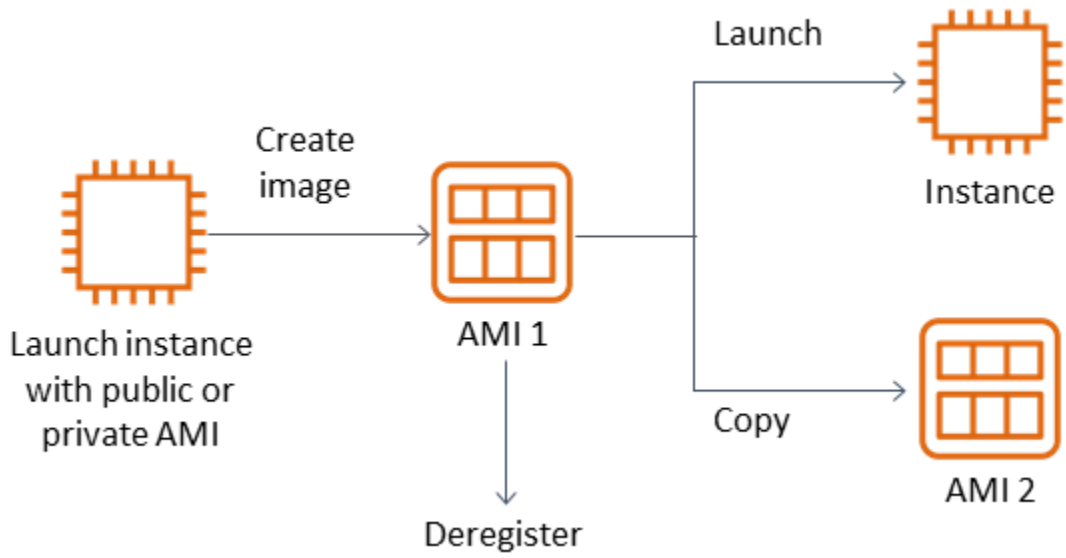
Introduzca una descripción y añada las etiquetas correspondientes. Añada una etiqueta `Name` para que sea más fácil encontrar el volumen más adelante. Añada cualquier otra etiqueta adecuada en función de su estrategia de etiquetado.

Creación de AMI

Una AMI proporciona la información necesaria para lanzar una instancia. La AMI incluye el volumen raíz y las instantáneas de los volúmenes de EBS adjuntos a la instancia cuando se creó la imagen. No puede lanzar nuevas instancias únicamente a partir de instantáneas de EBS; debe lanzar nuevas instancias desde una AMI.

Al crear una AMI, se crea en la cuenta y la región que esté utilizando. El proceso de creación de la AMI crea instantáneas de Amazon EBS para cada volumen adjunto a la instancia, y la AMI hace referencia a estas instantáneas de Amazon EBS. Estas instantáneas se encuentran en Amazon S3 y son muy duraderas.

Después de crear una AMI de su instancia de EC2, puede utilizar la AMI para volver a crear la instancia o lanzar más copias de la instancia. También puede copiar las AMI de una región a otra para la migración de aplicaciones o la recuperación de desastres (DR).



Se debe crear una AMI a partir de una instancia EC2, a menos que vaya a migrar una máquina virtual, como una máquina virtual VMWARE, a. AWS Para crear una AMI desde la consola Amazon EC2, seleccione la instancia, elija Acciones, elija Imagen y, a continuación, elija Crear imagen.

Amazon Data Lifecycle Manager

Puede utilizar Amazon Data Lifecycle Manager para automatizar la creación, retención y eliminación de instantáneas de EBS y las AMI respaldadas por EBS. La administración de instantáneas automatizadas le ayuda a hacer lo siguiente:

- Proteger datos valiosos aplicando una programación periódica de copias de seguridad
- Conservar las copias de seguridad de acuerdo con los requisitos de los auditores o las políticas internas de conformidad
- Reducir los costos de almacenamiento al eliminar las copias de seguridad obsoletas

Con Amazon Data Lifecycle Manager, puede automatizar el proceso de administración de instantáneas para las instancias EC2 (y sus volúmenes de EBS adjuntos) o volúmenes de EBS independientes. Admite opciones como la copia entre regiones, por lo que puede copiar las instantáneas automáticamente a otras regiones. AWS Copiar instantáneas a regiones alternativas es una forma de apoyar los esfuerzos de recuperación de desastres y restaurar las opciones en una región alternativa. También puede usar Amazon Data Lifecycle Manager para crear una política de ciclo de vida de instantáneas que permita la restauración rápida de instantáneas.

Amazon Data Lifecycle Manager es una característica incluida en Amazon EC2 y Amazon EBS. El uso de Amazon Data Lifecycle Manager es gratuito.

AWS Backup

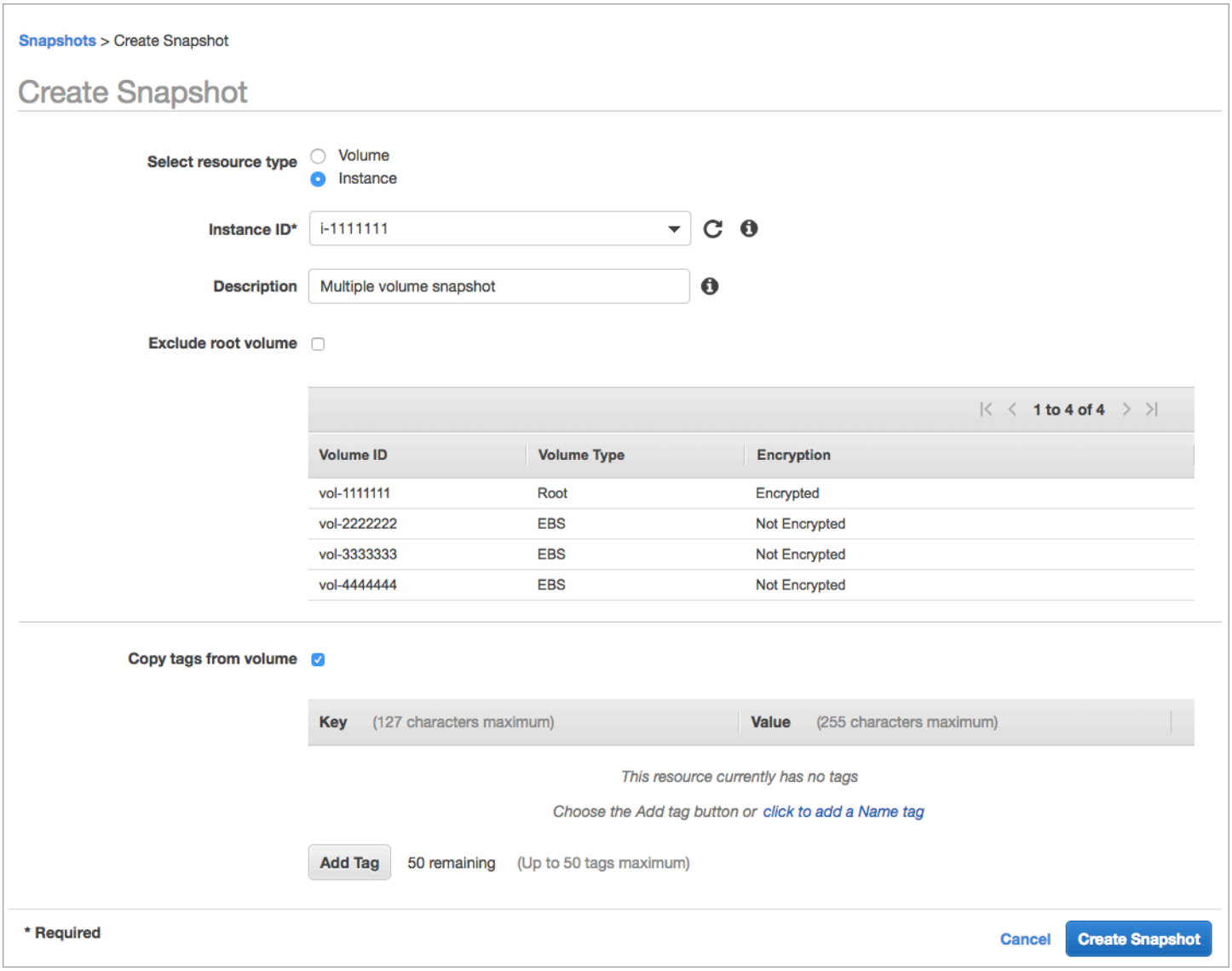
AWS Backup es exclusivo de Amazon Data Lifecycle Manager porque permite crear un plan de backup que incluya recursos de varios AWS servicios. Puede coordinar la copia de seguridad para cubrir los recursos que utiliza en conjunto, en lugar de coordinar las copias de seguridad de los recursos de forma individual.

AWS Backup también incluye el concepto de bóvedas de respaldo, que pueden restringir el acceso a los puntos de recuperación de las copias de seguridad completadas. Las operaciones de restauración se pueden iniciar desde cada recurso individual, AWS Backup en lugar de continuar con cada recurso individual y restaurar la copia de seguridad creada. AWS Backup también incluye una serie de funciones adicionales, como la gestión de auditorías y la elaboración de informes. Para obtener más información, consulte la sección Copia de seguridad y recuperación mediante AWS Backup de esta guía.

Realización de copias de seguridad de varios volúmenes

Si desea realizar una copia de seguridad de los datos de los volúmenes de EBS en una matriz de RAID utilizando instantáneas, estas deben ser coherentes. Esto se debe a que las instantáneas de estos volúmenes se crean de manera independiente. La restauración de volúmenes de EBS en una matriz de RAID a partir de instantáneas que no están sincronizadas daña la integridad de la matriz.

Para crear un conjunto coherente de instantáneas para su matriz RAID, utilice la operación de CreateSnapshotsAPI o inicie sesión en la consola Amazon EC2 y elija Elastic Block Store, Snapshots, Create Snapshot.



Las instantáneas de las instancias que tienen varios volúmenes conectados en una configuración RAID se toman como instantáneas de varios volúmenes, de forma colectiva. Las instantáneas de varios volúmenes proporcionan point-in-time instantáneas coordinadas por los datos y consistentes en fallos de varios volúmenes de EBS conectados a una instancia de EC2. Como las instantáneas se generan automáticamente en varios volúmenes de EBS, no tiene que detener la instancia para coordinar entre volúmenes para alcanzar la coherencia. Una vez iniciada la instantánea de los volúmenes (normalmente uno o dos segundos), el sistema de archivos puede continuar con sus operaciones.

Después de crear las instantáneas, cada una de ellas se trata como una instantánea individual. Puede realizar todas las operaciones de instantánea, como la restauración, la eliminación y la copia entre regiones y cuentas, como lo haría con una instantánea de un solo volumen. También puede etiquetar las instantáneas de varios volúmenes como lo haría con una única instantánea de volumen. Le recomendamos que etiquete sus instantáneas de varios volúmenes para gestionarlas de manera conjunta durante el proceso de restauración, copia o retención. Para obtener más información, consulte la documentación de AWS.

También puede realizar estas copias de seguridad desde un administrador de volúmenes lógico o una copia de seguridad a nivel de sistema de archivos. En estos casos, el uso de un agente de copias de seguridad tradicional permite hacer copias de seguridad de los datos a través de la red. Hay varias soluciones de copias de seguridad basadas en agentes disponibles en Internet y en el. AWS Marketplace

Un enfoque alternativo consiste en crear una réplica de los volúmenes principales del sistema que existen en un único volumen grande. Esto simplifica el proceso de copia de seguridad, ya que solo se debe realizar una copia de seguridad de un volumen grande y la copia de seguridad no se realiza en el sistema principal. Sin embargo, primero determine si el volumen individual puede funcionar lo suficiente durante la copia de seguridad y si el tamaño máximo del volumen es adecuado para la aplicación.

Proteger sus copias de seguridad de Amazon EC2

Es importante tener en cuenta la seguridad de las copias de seguridad y evitar su eliminación accidental o malintencionada. Puede utilizar varios enfoques de forma colectiva para lograrlo. Para evitar la pérdida de sus copias de seguridad críticas debido a una violación de seguridad, le recomendamos que las copie a otra cuenta. AWS Si tiene varias cuentas de AWS, puede designar una cuenta independiente como cuenta de archivo en la que todas las demás cuentas puedan copiar las copias de seguridad. Por ejemplo, puede hacerlo con una copia de seguridad multicuenta en AWS Backup.

Su plan de recuperación de desastres también puede requerir que sea capaz de reproducir instancias EC2 en otra región de AWS en caso de un fallo regional. Puede cumplir este objetivo copiando sus copias de seguridad en otra región dentro de la misma cuenta. Esto puede proporcionar un nivel adicional de protección contra la eliminación accidental y respaldar los objetivos de recuperación de desastres (DR). AWS Backup ofrece soporte para copias de seguridad entre regiones.

Considere bloquear los permisos de IAM para las acciones ec2: DeleteSnapshot y ec2:. DeregisterImage En su lugar, puede dejar que sus políticas y métodos de retención administren el ciclo de vida de las instantáneas de EBS y las AMI de Amazon EC2. Bloquear las acciones de eliminación es una forma de implementar una estrategia de escritura única y lectura múltiple (WORM) para las instantáneas de EBS. También puede usar AWS Backup Vault Lock, que proporciona soporte para instantáneas de EBS y otros recursos. AWS

Además, considere bloquear la posibilidad de que los usuarios compartan las AMI y las instantáneas de EBS bloqueando las acciones ec2: ModifyImageAttribute y ec2: IAM. ModifySnapshotAttribute Esto evitará que las AMI y las instantáneas se compartan con AWS cuentas externas a su organización. Si las utiliza AWS Backup, limite la posibilidad de que los usuarios realicen operaciones similares en los almacenes de respaldo. Para obtener más información, consulte la sección AWS Backup de esta guía.

Amazon EC2 incluye una característica de papelera de reciclaje que puede ayudarle a restaurar las instantáneas de EBS eliminadas accidentalmente. Si permite a sus usuarios eliminar las instantáneas, active esta característica para que las instantáneas necesarias no se eliminen permanentemente. Los usuarios deben tener especial cuidado al eliminar varias instantáneas, ya que la consola Amazon EC2 permite seleccionar varias instantáneas y eliminarlas en una sola operación. Además, tenga cuidado al utilizar los scripts de limpieza y la automatización para no eliminar involuntariamente las instantáneas que necesite. La característica de papelera de reciclaje ayuda a brindar protección contra este tipo de situaciones.

Archivado de instantáneas de EBS

Archivar las instantáneas de EBS puede ser un método rentable para conservar una copia de un volumen con fines de referencia que no vaya a restaurar durante 90 días o más. Este puede ser un buen paso intermedio antes de eliminar permanentemente todas las instantáneas relacionadas con un volumen de EBS. Por ejemplo, podría considerar archivar las instantáneas como un end-of-lifecycle paso para los volúmenes de EBS que ya no se utilizan. Archivar, en lugar de eliminarlas, también puede ser un método más rentable de eliminación y retención en lugar de utilizar la papelera de reciclaje.

Automatizar la creación de instantáneas y AMI con Systems Manager AWS CLI, el y los SDK AWS

Su enfoque de copia de seguridad puede requerir operaciones antes y después de crear una instantánea o una AMI. Por ejemplo, es posible que necesite parar e iniciar los servicios para

poner en reposo el sistema de archivos. O puede que tenga que detener e iniciar la instancia durante la creación de la AMI. Es posible que también necesite crear copias de seguridad de varios componentes de su arquitectura de forma conjunta, cada una con sus propios pasos previos y posteriores a la creación.

Puede reducir los plazos de mantenimiento de las copias de seguridad automatizando el proceso y verificando que el proceso de copia de seguridad se aplique de forma coherente. Para automatizar sus operaciones personalizadas previas y posteriores a la creación, programe el proceso de copia de seguridad mediante el SDK y el AWS CLI mismo.

La automatización se puede definir en un manual de procedimientos de Systems Manager que se puede ejecutar bajo demanda o durante un período de mantenimiento de Systems Manager. Puede conceder a sus usuarios acceso para ejecutar los manuales de ejecución de Systems Manager sin necesidad de concederles permisos para ejecutar comandos disruptivos de Amazon EC2. Esto también puede ayudarle a comprobar que los usuarios aplican el proceso de copia de seguridad y las etiquetas de forma coherente. Puede usar los CreateImage manuales de AWS CreateSnapshot y AWS para crear instantáneas y AMI, o puede conceder permisos a otros usuarios para que las usen. Systems Manager también incluye los UpdateWindowsAmi manuales de instrucciones de AWS UpdateLinuxAmi y AWS para automatizar la creación de parches y la creación de AMI.

También puede utilizar AWS CLI y AWS Tools for Windows PowerShellpara automatizar el proceso de creación de instantáneas y AMI. Puede usar el AWS CLI comando aws ec2 create-snapshot para crear una instantánea de un volumen de EBS como un paso de la automatización. Puede utilizar el comando aws ec2 create-snapshots para crear instantáneas sincronizadas y coherentes ante bloqueos de todos los volúmenes adjuntos a su instancia de EC2.

Puede usar la AWS CLI para crear nuevas AMI. Puede usar el comando aws ec2 register-image para crear una nueva imagen para la instancia de EC2. Para automatizar el cierre, la creación de imágenes y el reinicio de las instancias, combine este comando con los comandos aws ec2 stop-instances y aws ec2 start-instances.

Restauración de un volumen de Amazon EBS o una instancia EC2

Si necesita restaurar solo un volumen adjunto a una instancia de EC2, puede restaurar ese volumen por separado, separar el volumen existente y adjuntar el volumen restaurado a la instancia de EC2. Si necesita restaurar una instancia EC2 completa, incluidos todos sus volúmenes asociados, debe utilizar una copia de seguridad de imagen de máquina de Amazon (AMI) de la instancia.

Para reducir el tiempo de recuperación y el impacto en las aplicaciones y los procesos dependientes, el proceso de restauración debe tener en cuenta el recurso que está sustituyendo. Para obtener los mejores resultados, pruebe periódicamente el proceso de restauración en entornos de bajo nivel (por ejemplo, en entornos que no sean de producción) para comprobar que el proceso cumple con el objetivo de punto de recuperación (RPO) y el objetivo de tiempo de recuperación (RTO) y que el proceso de restauración funciona según lo esperado. Tenga en cuenta cómo afectará el proceso de restauración a las aplicaciones y los servicios que dependen de la instancia que vaya a restaurar y, a continuación, coordine la restauración según sea necesario. Intente automatizar y probar el proceso de restauración en la medida de lo posible para reducir el riesgo de que el proceso de restauración falle o se implemente de manera incoherente.

Si usa Elastic Load Balancing, con varias instancias que atienden el tráfico, puede dejar fuera de servicio una instancia defectuosa o con errores. A continuación, puede restaurar una nueva instancia para sustituirla mientras las demás instancias siguen prestando servicio al tráfico sin interrumpir a los usuarios.

Los siguientes procesos de restauración descritos son para instancias que no utilizan Elastic Load Balancing:

- Restauración de archivos y directorios individuales a partir de instantáneas de EBS
- Restauración de un volumen de EBS desde una instantánea de Amazon EBS
- Creación o restauración de una instancia EC2 desde una instantánea de EBS
- Restauración de una instancia en ejecución desde una AMI

Restauración de archivos y directorios a partir de instantáneas de EBS

Las instantáneas de EBS proporcionan una réplica point-in-time exacta del volumen original que se utilizó para crear la instantánea. Para restaurar archivos o directorios individuales, se debe hacer lo siguiente:

1. En primer lugar, restaure el volumen a partir de la instantánea de EBS que contiene los archivos o directorios.
2. Adjuntar el volumen a la instancia de EC2 en la que desea restaurar los archivos.
3. Copie los archivos del volumen restaurado al volumen de instancia de EC2.
4. Separe y elimine el volumen restaurado.

Restauración de un volumen de EBS desde una instantánea de Amazon EBS

Puede restaurar un volumen adjunto a una instancia EC2 existente creando un volumen a partir de su instantánea y adjuntándolo a su instancia. Puede utilizar las operaciones de consola, API o API para crear un volumen a partir de una instantánea existente. AWS CLI A continuación, puede montar el volumen en la instancia mediante el sistema operativo.

Tenga en cuenta que los datos de una instantánea de Amazon EBS se cargan de forma asíncrona en un volumen de EBS. Si una aplicación accede al volumen en el que no se cargan los datos, se produce una latencia más alta de lo normal mientras se cargan los datos desde Amazon S3. Para evitar este impacto en aplicaciones con sensibilidad a la latencia, dispone de dos opciones:

- Puede inicializar el volumen de EBS.
- Por un cargo adicional, Amazon EBS admite la restauración rápida de instantáneas, lo que elimina la necesidad de inicializar el volumen.

Si va a sustituir un volumen que debe utilizar el mismo punto de montaje, desmonte ese volumen para poder montar el nuevo volumen en su lugar. Para desmontar el volumen, detenga primero todos los procesos que estén utilizando el volumen. Si va a reemplazar el volumen raíz, debe parar primero la instancia antes de poder separar el volumen raíz.

Por ejemplo, siga estos pasos para restaurar un volumen a una point-in-time copia de seguridad anterior mediante la consola:

1. En la consola de Amazon EC2, en el menú Elastic Block Store, elija Instantáneas.
2. Busque la instantánea que desea restaurar y selecciónela.
3. Elija Acciones y, a continuación, seleccione Crear volumen.
4. Cree el nuevo volumen en la misma zona de disponibilidad que su instancia EC2.
5. Abra la consola de Amazon EC2 y seleccione la instancia.
6. En los detalles de la instancia, anote el nombre del dispositivo que desea reemplazar en la entrada dispositivo raíz o dispositivos de bloques.
7. Retire el volumen. El proceso es diferente para los volúmenes raíz y los volúmenes no raíz.

   Para volúmenes raíz:

   a. Detenga la instancia EC2.

b. En el menú de volúmenes de Elastic Block de EC2, seleccione el volumen raíz que desee reemplazar.
c. Elija Acciones y a continuación seleccione Desvincular volumen.
d. En el menú de volúmenes de Elastic Block de EC2, seleccione el nuevo volumen que desea reemplazar.
e. Elija Acciones y, a continuación, elija Adjuntar volumen.
f. Seleccione la instancia a la que desee adjuntar el volumen y utilice el mismo nombre de dispositivo que indicó anteriormente.

Para volúmenes que no son raíz:

a. En el menú de volúmenes de Elastic Block de EC2, seleccione el volumen que no son raíz que desee reemplazar.
b. Elija Acciones y a continuación seleccione Desvincular volumen.
c. Adjunte el nuevo volumen seleccionándolo en el menú de EC2 Elastic Block Store Volumes y, a continuación, seleccione Acciones, Adjuntar volumen. Seleccione la instancia a la que desee adjuntarlo y, a continuación, seleccione un nombre de dispositivo disponible.
d. Con el sistema operativo de la instancia, desmonte el volumen existente y, a continuación, monte el nuevo volumen en su lugar.

   En Linux, puede utilizar el comando `umount`. En Windows, puede usar un administrador de volúmenes lógicos (LVM), como la utilidad del sistema Disk Management.
e. Separe los volúmenes anteriores que desee sustituir seleccionándolos en el menú de EC2 Elastic Block Store Volumes y, a continuación, seleccione Acciones, Desvincular volumen.

También puede utilizarla AWS CLI en combinación con los comandos del sistema operativo para automatizar estos pasos.

Creación o restauración de una instancia EC2 desde una instantánea de EBS

Para crear una copia de seguridad que se utilizará para restaurar una instancia de EC2 completa, se recomienda crear una imagen de máquina de Amazon (AMI). Las AMI capturan información de la máquina, como el tipo de virtualización. También crean instantáneas para cada volumen adjunto a la instancia EC2, incluidas las asignaciones de sus dispositivos, de modo que se puedan restaurar en la misma configuración.

Sin embargo, si debe utilizar una instantánea de EBS para restaurar una instancia, cree primero una AMI a partir de una instantánea de EBS que se convertirá en el volumen raíz de la nueva instancia de EC2:

1. En la consola de Amazon EC2, en el menú Elastic Block Store, elija Instantáneas.
2. Busque la instantánea que se utilizará para crear el volumen raíz de la nueva instancia EC2 y selecciónela.
3. Seleccione la instantánea y elija Acciones, Crear imagen.
4. Introduzca un nombre para la imagen (por ejemplo,`YYYYMMDD-restore-for-i-012345678998765de`) y elija las opciones adecuadas para la nueva imagen.

Una vez que la imagen esté creada y esté disponible, puede lanzar una nueva instancia de EC2 que utilizará la instantánea de EBS como volumen raíz.

Restauración de una instancia en ejecución desde una AMI

Puede abrir una nueva instancia desde la copia de seguridad de la AMI para reemplazar una instancia existente que esté en ejecución. Un enfoque consiste en detener la instancia existente, mantenerla sin conexión mientras lanza una nueva instancia desde la AMI y realizar las actualizaciones necesarias. Este enfoque reduce el riesgo de conflictos si ambas instancias se ejecutan simultáneamente. Es un enfoque aceptable si los servicios que proporciona la instancia no funcionan o si se realiza la restauración durante un período de mantenimiento. Después de probar la nueva instancia, puede reasignar cualquier dirección IP elástica que se haya asignado a la instancia anterior. A continuación, puede actualizar cualquier registro del Servicio de nombres de dominio (DNS) para que apunte a la nueva instancia.

Sin embargo, si durante una restauración debe minimizar el tiempo de inactividad de la instancia en servicio, considere lanzar y probar una nueva instancia desde la copia de seguridad de la AMI. A continuación, reemplace la instancia existente por la nueva instancia.

Mientras ambas instancias estén en ejecución, debe evitar que la nueva instancia provoque colisiones a nivel de plataforma o de aplicación. Por ejemplo, es posible que tenga problemas con las instancias de Windows unidas a un dominio que se ejecutan con el mismo SID y el mismo nombre de equipo. Es posible que tenga problemas similares con las aplicaciones y los servicios de red que requieren identificadores únicos.

Para evitar que otros servidores y servicios se conecten a la nueva instancia antes de que esté lista, use grupos de seguridad para bloquear temporalmente todas las conexiones entrantes de

la nueva instancia, excepto la de su propia dirección IP, para acceder a ella y realizar pruebas. También puede bloquear temporalmente las conexiones salientes de la nueva instancia para evitar que los servicios y las aplicaciones inicien conexiones o actualizaciones a otros recursos. Cuando la nueva instancia esté lista, detenga la instancia existente, inicie los servicios y procesos en la nueva instancia y, a continuación, desbloquee cualquier conexión de red entrante o saliente que haya implementado.

Copia de seguridad y recuperación desde la infraestructura en las instalaciones hasta AWS

Puede utilizarlos AWS para almacenar de forma duradera y remota las copias de seguridad de su infraestructura local. Al utilizar los servicios AWS de almacenamiento en este escenario, puede centrarse en las tareas de copia de seguridad y archivado. No tiene que preocuparse por el aprovisionamiento, el escalado o la capacidad de la infraestructura de almacenamiento para sus tareas de copia de seguridad.

Amazon S3 ofrece amplias operaciones de API y SDK para integrarlos en sus enfoques de respaldo y recuperación nuevos y existentes. Esto también ofrece a los proveedores de software de respaldo formas de integrar directamente sus aplicaciones con las soluciones AWS de almacenamiento.

En este escenario, el software de backup y archivado que utiliza en su infraestructura local interactúa directamente AWS a través de las operaciones de la API. Como el software de copia AWS de seguridad es compatible con los datos, realiza copias de seguridad de los datos de los servidores locales directamente en Amazon S3.

Si tu software de backup actual no es compatible de forma nativa con la AWS nube, puedes usar Storage Gateway. Storage Gateway, un servicio de almacenamiento en la nube, proporciona a sus sistemas en las instalaciones acceso a un almacenamiento en la nube escalable. Es compatible con protocolos de almacenamiento estándar abiertos que funcionan con sus aplicaciones existentes y, al mismo tiempo, almacenan de forma segura sus datos cifrados en Amazon S3. Puede usar Storage Gateway como parte de un enfoque de respaldo y recuperación para sus cargas de trabajo de almacenamiento basadas en bloques en las instalaciones.

Storage Gateway resulta útil en situaciones híbridas en las que desea realizar la transición a un almacenamiento basado en la nube para sus copias de seguridad. Storage Gateway también le ayuda a reducir las inversiones de capital en almacenamiento en las instalaciones. Se implementa Storage Gateway como una máquina virtual o un dispositivo de hardware dedicado. Esta guía se centra en cómo Storage Gateway se aplica al copia de seguridad y la recuperación.

Storage Gateway ofrece tres opciones diferentes para satisfacer distintos requisitos:

- Una puerta de enlace de archivos para almacenar archivos de datos de aplicaciones e imágenes de respaldo como objetos duraderos en el almacenamiento en la nube Amazon S3 mediante un acceso basado en SMB o NFS.

- Una puerta de enlace de volúmenes para presentar volúmenes de almacenamiento en bloques iSCSI basados en la nube a sus aplicaciones en las instalaciones. Una puerta de enlace de volumen proporciona una caché local o volúmenes completos en las instalaciones y, al mismo tiempo, almacena copias completas de los volúmenes en la nube de AWS .
- Una puerta de enlace de cinta para dirigir un software de respaldo confiable a una puerta de enlace de almacenamiento local que, a su vez, se conecta a Amazon S3. Esta opción ofrece la escalabilidad y la durabilidad de la nube para una retención segura y a largo plazo sin interrumpir las inversiones o los procesos existentes.

Puerta de enlace de archivo

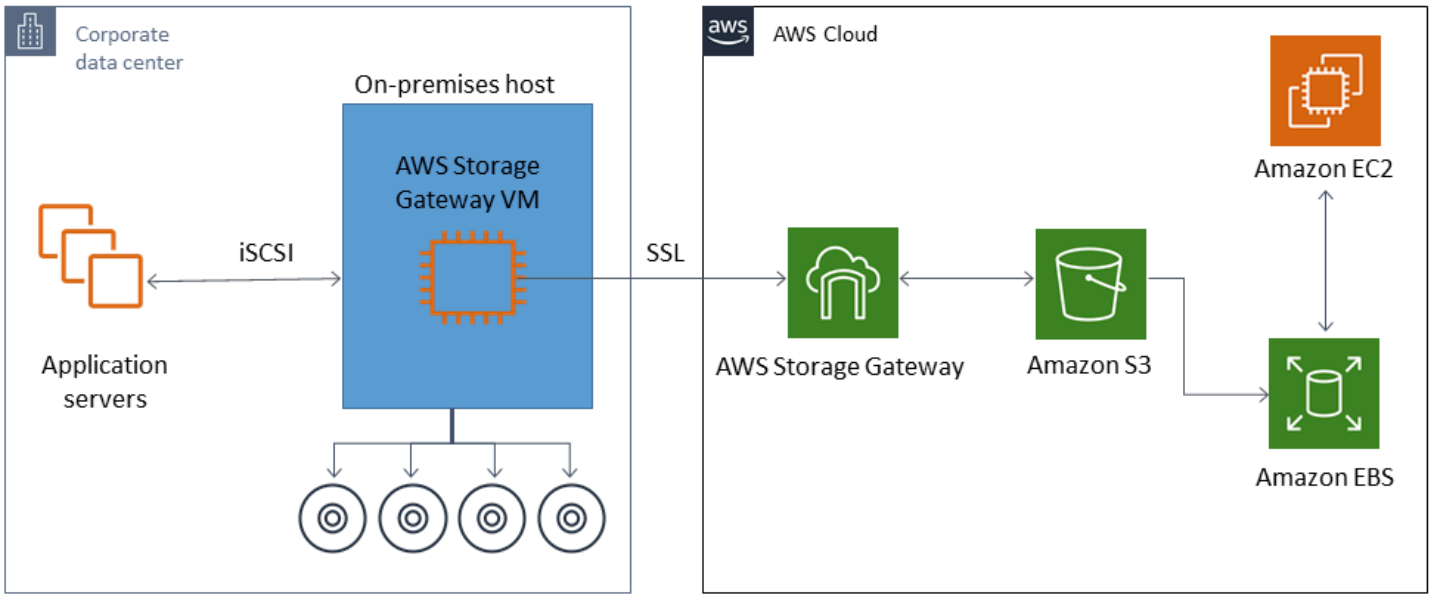
Muchas organizaciones comienzan su traspaso a la nube trasladando datos secundarios y terciarios, como las copias de seguridad, a la nube. La compatibilidad con interfaces SMB y NFS de una puerta de enlace de archivos ofrece a los grupos de TI una forma de realizar la transición de los trabajos de copia de seguridad de los sistemas de copia de seguridad en las instalaciones existentes a la nube. Las aplicaciones de copia de seguridad, las herramientas de bases de datos nativas o los scripts que pueden escribir en SMB o NFS pueden escribir en una puerta de enlace de archivos. La puerta de enlace de archivo almacena las copias de seguridad como objetos de Amazon S3 de hasta 5 TiB de tamaño. Con una caché local del tamaño adecuado, las copias de seguridad recientes se pueden utilizar para realizar recuperaciones rápidas en las instalaciones. Las necesidades de retención a largo plazo se abordan mediante la organización por niveles de las copias de seguridad en las clases de almacenamiento S3 Standard-Infrequent Access y S3 Glacier de bajo costo.

La puerta de enlace de archivos proporciona una vía de acceso para su almacenamiento basado en bloques a Amazon S3 para realizar copias de seguridad externas de gran durabilidad. Resulta especialmente útil en situaciones en las que es necesario restaurar rápidamente un archivo del que se ha hecho una copia de seguridad reciente. Como una puerta de enlace de archivos admite los protocolos SMB y NFS, los usuarios pueden acceder a los archivos de la misma forma que accederían a un recurso compartido de archivos de la red. Igualmente, puede aprovechar las ventajas de las capacidades de control de versiones de objetos de Amazon S3. Con el control de versiones de objetos, puede restaurar las versiones anteriores de los objetos de un archivo y, a continuación, acceder a ellas fácilmente mediante SMB o NFS.

Puerta de enlace de volumen

Una puerta de enlace de volumen le permite aprovisionar volúmenes de almacenamiento en bloques iSCSI basados en la nube para sus servidores en las instalaciones. La puerta de enlace

de volumen almacena los datos de volumen en Amazon S3 para un almacenamiento externo duradero y escalable basado en la nube. Una pasarela de volúmenes facilita la toma de point-in-time instantáneas completas de sus volúmenes y su almacenamiento en la nube como instantáneas de Amazon EBS. Una vez guardados como instantáneas, los volúmenes completos se pueden restaurar como volúmenes de EBS y adjuntarlos a instancias de EC2, lo que agiliza una solución de recuperación de desastres basada en la nube. Los volúmenes también se pueden restaurar en Storage Gateway, lo que permite que las aplicaciones en las instalaciones vuelvan a un estado anterior.



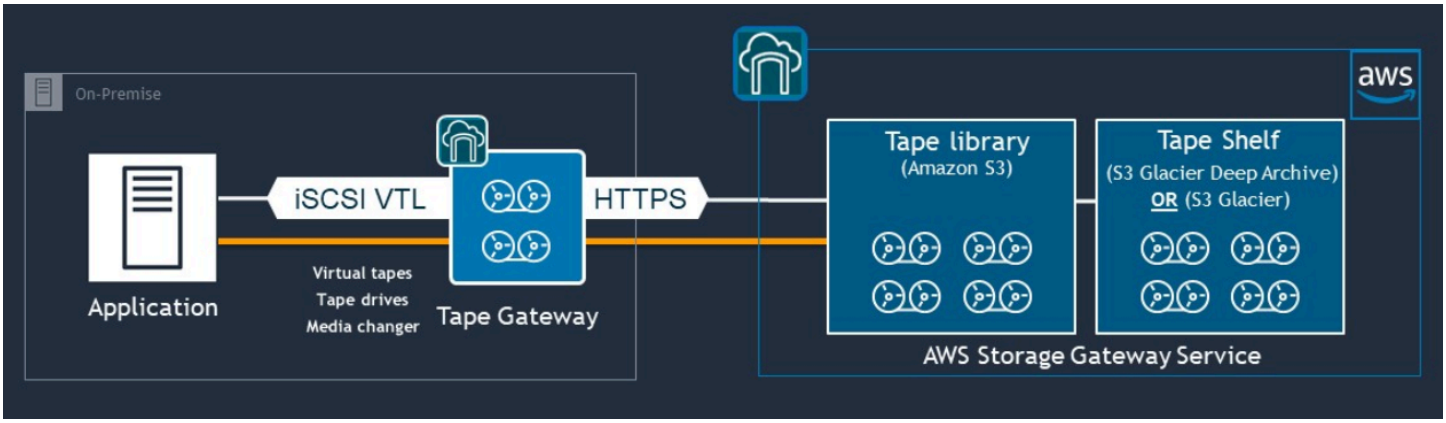
Como una pasarela de volúmenes se integra con la función de volumen de Amazon EBS de Amazon EC2, puede AWS Backup utilizarla para automatizar y programar el proceso de instantáneas. Una puerta de enlace de volumen le proporciona las ventajas adicionales de contar con características de etiquetado e instantáneas duraderas de Amazon EBS respaldadas por Amazon S3. Para obtener más información, consulte la Documentación gráfica de Amazon EBS.

Puerta de enlace de cinta

Una puerta de enlace de cinta ofrece la alta durabilidad, el almacenamiento en niveles de bajo costo y las amplias funciones de Amazon S3 para su almacén de copias de seguridad en cinta virtual externo. Todas las cintas virtuales almacenadas en Amazon S3 se replican y almacenan en al menos tres zonas de disponibilidad dispersas geográficamente. Sus cintas virtuales están protegidas por una durabilidad de 11 nueves.

AWS también realiza comprobaciones de estabilidad de forma periódica para confirmar que sus datos se pueden leer y que no se ha introducido ningún error. Todas las cintas almacenadas en Amazon S3 están protegidas mediante cifrado del lado del servidor mediante claves predeterminadas o sus AWS KMS claves. Además, evita los riesgos de seguridad física asociados a la portabilidad de las cintas. Con una puerta de enlace de cintas, obtiene los datos correctos, en comparación con el almacenamiento externo de cintas, donde podría recibir una cinta incorrecta o rota durante la restauración.

Puede ahorrar en los costos de almacenamiento mensuales al almacenar sus datos en Amazon S3. Puede ahorrar aún más para sus necesidades de archivado a largo plazo con el archivo profundo de S3 Glacier.



Una puerta de enlace de cintas actúa como una biblioteca de cintas virtual (VTL) que abarca desde su entorno en las instalaciones hasta servicios de almacenamiento altamente escalables, redundantes y duraderos: Amazon S3, Recuperación flexible de S3 Glacier y Archivo profundo de S3 Glacier.

La puerta de enlace de cintas presenta a Storage Gateway a su aplicación de copia de seguridad existente como una VTL basada en iSCSI de estándar abierto, con un cambiador de medios virtuales y unidades de cinta virtuales. Puede seguir utilizando sus flujos de trabajo y aplicaciones de copia de seguridad existentes mientras escribe en un conjunto de cintas virtuales almacenadas en Amazon S3 con escalabilidad masiva. Cuando ya no necesite un acceso inmediato o frecuente a los datos de una cinta virtual, su aplicación de copia de seguridad puede archivarlos en Recuperación flexible de S3 Glacier o Archivo profundo de S3 Glacier, lo que reduce aún más los costos de almacenamiento.

Por lo general, puede recuperar una cinta que esté archivada en Recuperación flexible de S3 Glacier o Archivo profundo de S3 Glacier en un plazo de 3 a 5 o 12 horas, respectivamente. La puerta de enlace de cintas se puede usar con una aplicación de respaldo que sea compatible con la interfaz de biblioteca de cintas basada en iSCSI para acceder a las cintas virtuales. Tenga en cuenta también el

tamaño mínimo de almacenamiento de 100 GB por cinta. Para obtener más información, consulte la lista de aplicaciones de respaldo de terceros que admiten puertas de enlace de cinta.

Copia de seguridad y recuperación de aplicaciones de AWS a su centro de datos

Es posible que tenga una política que exija implementar un escenario como la recuperación ante desastres o la continuidad empresarial para sus cargas de trabajo basadas en la nube y su infraestructura local. Si ya dispone de un marco de copias de seguridad de datos para sus servidores en las instalaciones, puede ampliarlo a sus recursos AWS a través de una conexión VPN o mediante AWS Direct Connect. Puede instalar el agente de copias de seguridad en las instancias EC2 y hacer copias de seguridad de sus datos y aplicaciones de acuerdo con sus políticas de protección de datos. También puede utilizar Amazon S3 como servicio intermedio para almacenar sus copias de seguridad a nivel de aplicación. A continuación, puede utilizar las operaciones de la API, los SDK o AWS CLI para restaurar los datos en su entorno en las instalaciones.

Para hacer copias de seguridad de los datos en servicios AWS distintos de Amazon EC2, utilice AWS CLI, los SDK y las operaciones de API para extraer los datos en el formato que desee. A continuación, copie los datos en Amazon S3, y cópielos también de Amazon S3 a su entorno en las instalaciones. Algunos servicios ofrecen exportación directa a Amazon S3. Por ejemplo, Amazon RDS admite la copia de seguridad nativa de las bases de datos de Microsoft SQL Server en Amazon S3.

Copia de seguridad y recuperación de servicios de AWS nativos en la nube

Su método de copia de seguridad y recuperación debe abarcar los servicios de AWS que se utilizan en sus cargas de trabajo. AWS proporciona características y opciones específicas del servicio para administrar sus datos e interactuar con ellos. Puede usar la consola, la AWS CLI, los SDK y las operaciones de la API para implementar la copia de seguridad y la recuperación de los servicios de AWS que esté utilizando. En esta guía se describe Amazon RSD y Amazon DynamoDB como ejemplos. AWS Backup es compatible con DynamoDB y Amazon RSD y se debe utilizar si cumple sus requisitos.

Copia de seguridad y recuperación para Amazon RSD

Amazon RDS incluye características para automatizar copias de seguridad de las bases de datos. Amazon RDS crea una instantánea del volumen de almacenamiento de su instancia de base de datos, haciendo una copia de seguridad de toda la instancia de base de datos, no solo de bases de datos individuales. Con Amazon RDS, puede establecer una ventana de copia de seguridad para realizar copias de seguridad automatizadas, crear instantáneas de instancias de bases de datos y compartir y copiar instantáneas entre regiones y cuentas.

Amazon RDS ofrece dos opciones diferentes para realizar copias de seguridad y restaurar sus instancias de base de datos:

- Las copias de seguridad automatizadas proporcionan recuperación en un momento dado (PITR) de su instancia de base de datos. Las copias de seguridad automatizadas se activan de forma predeterminada cuando crea una nueva instancia de base de datos.

  Amazon RDS realiza una copia de seguridad diaria completa de sus datos durante un período que usted define al crear la instancia de base de datos. Puede configurar un período de retención de hasta 35 días para la copia de seguridad automatizada. Amazon RDS también carga los registros de transacciones de las instancias de base de datos en Amazon S3 cada 5 minutos. Amazon RDS utiliza las copias de seguridad diarias junto con los registros de transacciones de la base de datos para restaurar la instancia de base de datos. Puede restaurar la instancia en cualquier segundo durante el período de retención, hasta `LatestRestorableTime` (normalmente, los últimos cinco minutos).

Para encontrar el último tiempo restaurable de sus instancias de base de datos, utilice la llamada a la API `DescribeDBInstances`. O bien, busque la base de datos en la pestaña Descripción de la consola de Amazon RDS.

Al iniciar una PITR, los registros de transacciones se combinan con la copia de seguridad diaria más adecuada para restaurar la instancia de base de datos a la hora solicitada.

- Las instantáneas de base de datos son copias de seguridad iniciadas por el usuario que puede usar para restaurar la instancia de base de datos a un estado conocido con la frecuencia que desee. A continuación, podrá restaurarla a ese estado en cualquier momento. Puede utilizar la consola de Amazon RDS o la llamada a la API `CreateDBSnapshot` para generar instantáneas de bases de datos. Estas instantáneas se conservan hasta que utilice la consola o la llamada a la API `DeleteDBSnapshot` para eliminarlas de forma explícita.

Ambas opciones de copia de seguridad son compatibles con Amazon RDS en AWS Backup, que también ofrece otras características. Considere la posibilidad de utilizar AWS Backup para configurar un plan de copia de seguridad estándar para sus bases de datos de Amazon RDS y utilice las opciones de copia de seguridad de instancia iniciada por el usuario cuando sus planes de copia de seguridad para una base de datos en particular sean únicos.

Amazon RDS impide el acceso directo al almacenamiento subyacente que utiliza la instancia de base de datos. Esto también le impide exportar directamente la base de datos de una instancia de base de datos de RDS a su disco local. En algunos casos, puede utilizar las funciones nativas de copia de seguridad y restauración usando utilidades de cliente. Por ejemplo, puede usar el comando mysqldump con una base de datos MySQL de Amazon RDS para exportar una base de datos a su máquina cliente local. En algunos casos, Amazon RDS ofrece además opciones ampliadas para realizar una copia de seguridad y restauración nativas de una base de datos. Por ejemplo, Amazon RDS proporciona procedimientos almacenados para exportar e importar copias de seguridad de bases de datos RDS de bases de datos de SQL Server.

Asegúrese de probar minuciosamente el proceso de restauración de su base de datos y su impacto en los clientes de bases de datos como parte del método general de copia de seguridad y restauración.

Uso de registros CNAME de DNS para reducir el impacto en los clientes durante la recuperación de una base de datos

Al restaurar una base de datos mediante PITR o una instantánea de una instancia de base de datos RDS, se crea una nueva instancia de base de datos con un nuevo punto de conexión. De esta forma, puede crear varias instancias de base de datos a partir de una instantánea de base de datos o de un momento específico. Al restaurar una instancia de base de datos de RDS para reemplazar una instancia de base de datos de RDS activa, se deben tener en cuenta aspectos especiales. Por ejemplo, debe determinar cómo redirigirá los clientes de base de datos existentes a la nueva instancia con la mínima interrupción y modificación. También debe garantizar la continuidad y la coherencia de los datos de la base de datos teniendo en cuenta el tiempo de restauración de datos y el tiempo de recuperación cuando la nueva instancia comience a recibir escrituras.

Puede crear un registro CNAME de DNS independiente que apunte al punto de conexión de la instancia de base de datos y hacer que sus clientes usen este nombre de DNS. A continuación, puede actualizar el CNAME para que apunte a un nuevo punto de conexión restaurado sin tener que actualizar los clientes de la base de datos.

Establezca el tiempo de vida (TTL) de su registro CNAME en un valor adecuado. El TTL que especifique determina durante cuánto tiempo se guarda el registro en caché con los solucionadores de DNS antes de que se realice otra solicitud. Es importante tener en cuenta que es posible que algunos solucionadores o aplicaciones de DNS no respeten el TTL y almacenen en caché el registro durante más tiempo que el TTL. Para Amazon Route 53, si especifica un valor más largo (por ejemplo, 172800 segundos o dos días), se reduce el número de llamadas que los solucionadores recursivos de DNS deben realizar a Route 53 para obtener la información más reciente de este registro. Esto reduce la latencia y reduce su factura por el servicio de Route 53. Para obtener más información, consulte Cómo dirige Amazon Route 53 el tráfico de su dominio.

Las aplicaciones y los sistemas operativos de los clientes también pueden almacenar en caché la información de DNS que debe vaciar o reiniciar para iniciar una nueva solicitud de resolución de DNS y recuperar el registro CNAME actualizado.

Cuando inicie una restauración de base de datos y transfiera el tráfico a la instancia restaurada, compruebe que todos sus clientes escriben en la instancia restaurada y no en la anterior. Es posible que la arquitectura de datos permita restaurar la base de datos, actualizar el DNS para transferir el tráfico a la instancia restaurada y, posteriormente, corregir cualquier dato que aún se pueda estar escribiendo en la instancia anterior. Si no es así, puede detener la instancia existente antes de actualizar el registro CNAME de DNS. Entonces, todo el acceso proviene de la instancia recién

restaurada. Esto puede provocar temporalmente problemas de conexión de algunos de los clientes de la base de datos que puede gestionar de forma individual. Para reducir el impacto en el cliente, puede realizar la restauración de la base de datos durante un período de mantenimiento.

Diseñe sus aplicaciones para gestionar correctamente los errores de conexión a la base de datos con reintentos mediante retroceso exponencial. Esto permite que la aplicación se recupere cuando una conexión a la base de datos deje de estar disponible durante una restauración sin provocar que la aplicación se bloquee inesperadamente.

Una vez finalizado el proceso de restauración, puede mantener la instancia anterior en estado detenido. O bien, puede usar las reglas de los grupos de seguridad para limitar el tráfico a la instancia anterior hasta que esté convencido de que ya no es necesaria. Para adoptar un enfoque de desmantelamiento gradual, limite primero el acceso a una base de datos en ejecución mediante el grupo de seguridad. En un momento dado, puede detener la instancia cuando ya no sea necesaria. Por último, obtenga una instantánea de la instancia de la base de datos y elimínela.

Copia de seguridad y recuperación para DynamoDB

DynamoDB proporciona PITR, que realiza copias de seguridad casi continuas de los datos de tablas de DynamoDB. Cuando está habilitada, DynamoDB mantiene copias de seguridad incrementales de la tabla durante los últimos 35 días hasta que la desactive explícitamente.

También puede crear copias de seguridad a demanda de la tabla de DynamoDB mediante la consola de DynamoDB, AWS CLI o la API de DynamoDB. Para obtener más información, consulte Copia de seguridad de una tabla de DynamoDB. Puede programar copias de seguridad periódicas o futuras mediante AWS Backup, o puede personalizar y automatizar su método de copia de seguridad mediante funciones de Lambda. Para obtener más información sobre el uso de funciones de Lambda para realizar copias de seguridad de DynamoDB, consulte la publicación del blog Una solución sin servidor para programar su copia de seguridad bajo demanda de Amazon DynamoDB. Si no desea crear scripts de programación y trabajos de limpieza, puede utilizar AWS Backup para crear planes de copia de seguridad. Los planes de copias de seguridad incluyen programas y políticas de retención para las tablas de DynamoDB. AWS Backupcrea las copias de seguridad y elimina las copias de seguridad anteriores en función de su programa de retención. AWS Backup también incluye opciones avanzadas de copia de seguridad de DynamoDB que no están disponibles en el servicio DynamoDB, como almacenamiento por niveles de menor costo y copias entre cuentas y regiones. Para obtener más información, consulte Copia de seguridad avanzada de DynamoDB.

Debe configurar manualmente lo siguiente en una tabla de DynamoDB que se restaure:

- Políticas de escalado automático
- Políticas de IAM
- Alarmas y métricas de Amazon CloudWatch
- Etiquetas
- Ajustes de transmisión
- Configuración de TTL

Solo puede restaurar todos los datos de la tabla en una nueva tabla a partir de un backup. Solo puede escribir en la tabla restaurada después de que se active.

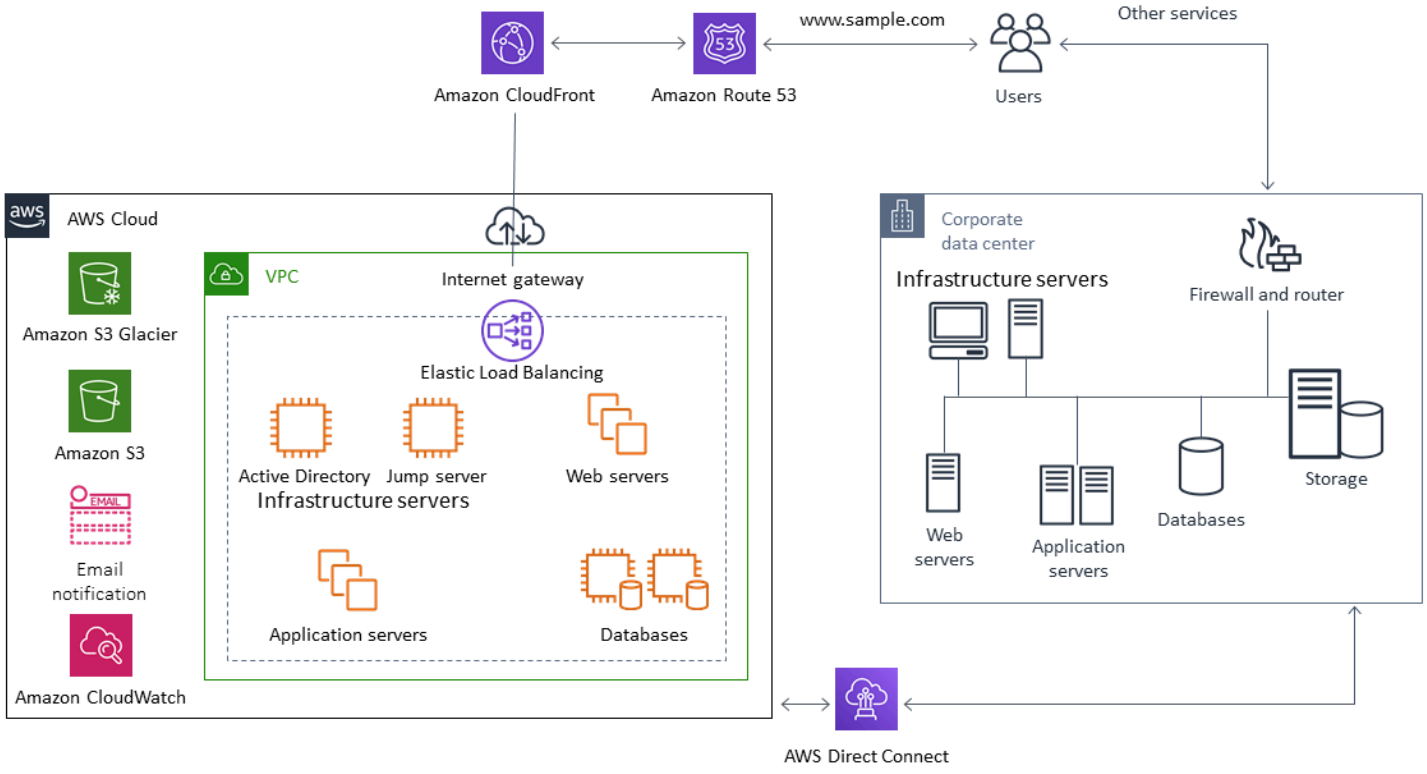
El proceso de restauración debe tener en cuenta cómo se indicará a los clientes que utilicen el nombre de la tabla recién restaurada. Puede configurar sus aplicaciones y clientes para que recuperen el nombre de la tabla de DynamoDB a partir de un archivo de configuración, un valor del Almacén de parámetros de AWS Systems Manager u otra referencia que se pueda actualizar dinámicamente para reflejar el nombre de la tabla que debe usar el cliente.

Como parte del proceso de restauración, debe considerar detenidamente el proceso de cambio. Puede optar por denegar el acceso a la tabla de DynamoDB existente mediante los permisos de IAM y permitir el acceso a la nueva tabla. A continuación, puede actualizar la configuración de la aplicación y el cliente para usar la nueva tabla. Es posible que también necesite conciliar las diferencias entre la tabla de DynamoDB existente y la tabla de DynamoDB recién restaurada.

Copia de seguridad y recuperación para arquitecturas híbridas

Las implementaciones locales y nativas de la nube que se describen en esta guía se pueden combinar en escenarios híbridos en los que el entorno de carga de trabajo tiene componentes locales y de infraestructura. AWS Los recursos, incluidos los servidores web, los servidores de aplicaciones, los servidores de supervisión, las bases de datos y Microsoft Active Directory, se alojan en el centro de datos del cliente o bien en AWS. Las aplicaciones que se ejecutan en la AWS nube están conectadas a las aplicaciones que se ejecutan en las instalaciones.

Este escenario es cada vez más habitual en cargas de trabajo empresariales. Muchas empresas tienen sus propios centros de datos y los utilizan AWS para aumentar la capacidad. Estos centros de datos de clientes suelen estar conectados a la AWS red mediante enlaces de red de alta capacidad. Por ejemplo, con AWS Direct Connect, puede establecer una conectividad privada y dedicada desde su centro de datos local a. AWS Esta opción proporciona el ancho de banda y la latencia coherente necesarios para cargar datos a la nube con fines de protección de datos. También proporciona un rendimiento y una latencia coherentes en cargas de trabajo híbridas. El siguiente diagrama muestra un ejemplo de enfoque de entorno híbrido.



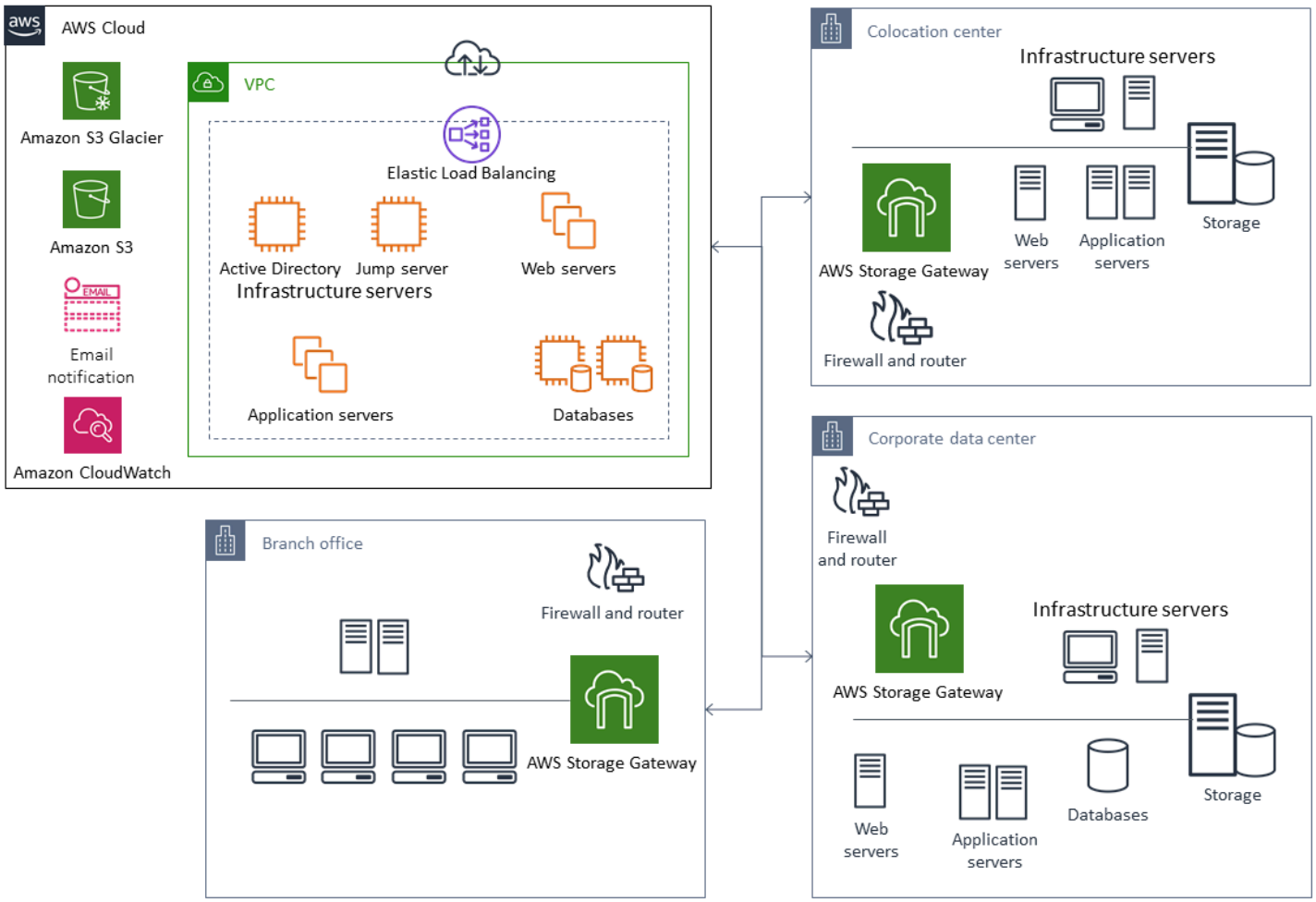
Las soluciones de protección de datos bien diseñadas suelen emplear una combinación de las opciones descritas en las soluciones para entornos en las instalaciones y nativos en la nube de esta guía. Muchos ISV que ofrecen soluciones de copia de seguridad y restauración líderes en el mercado para infraestructuras en las instalaciones las han ampliado para admitir enfoques híbridos.

Trasladar las soluciones de gestión de copias de seguridad centralizadas a la nube para aumentar la disponibilidad

Al utilizar sus inversiones en soluciones de administración de respaldo existentes AWS, puede mejorar la resiliencia y la arquitectura de su enfoque. Es posible que tenga un servidor de respaldo principal y uno o más servidores multimedia o de almacenamiento en las instalaciones, distribuidos en múltiples ubicaciones cerca de los servidores y servicios que protegen. En este caso, considere la posibilidad de trasladar el servidor de respaldo principal a una instancia de EC2 para protegerlo de posibles desastres en las instalaciones y lograr una alta disponibilidad.

Para gestionar los flujos de datos de copias de seguridad, puede crear uno o más servidores multimedia en instancias de EC2 de la misma región que los servidores que van a proteger. Los servidores multimedia cerca de las instancias de EC2 le permiten ahorrar dinero en las transferencias por internet. Al realizar copias de seguridad en Amazon S3, los servidores multimedia aumentan el rendimiento general de las copias de seguridad y recuperación.

También puede usar Storage Gateway para proporcionar acceso centralizado en la nube a los datos de centros de datos y oficinas geográficamente dispersos. Por ejemplo, una puerta de enlace de archivos le brinda acceso bajo demanda y de baja latencia a los datos almacenados en los flujos de trabajo de aplicaciones que pueden extenderse AWS por todo el mundo. Puede usar características como la actualización de caché para actualizar los datos en ubicaciones distribuidas geográficamente. Así, el contenido se puede compartir fácilmente entre las oficinas.


AWS Cloud
Amazon S3 Glacier
Amazon S3
Email notification
Amazon CloudWatch
VPC
Elastic Load Balancing
Active Directory
Jump server
Infrastructure servers
Web servers
Application servers
Databases
Colocation center
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Storage
Firewall and router
Corporate data center
Firewall and router
AWS Storage Gateway
Infrastructure servers
Web servers
Application servers
Databases
Storage
Branch office
Firewall and router
AWS Storage Gateway

Recuperación ante desastres con AWS

Los enfoques de respaldo y restauración y los servicios y tecnologías de apoyo se pueden utilizar para implementar su solución de recuperación de desastres (DR). Muchas empresas utilizan la AWS nube para realizar copias de seguridad y restauración y como sitio de recuperación ante desastres. AWS proporciona una serie de servicios y funciones que respaldan la recuperación ante desastres y la continuidad empresarial.

Temas

DR local para AWS

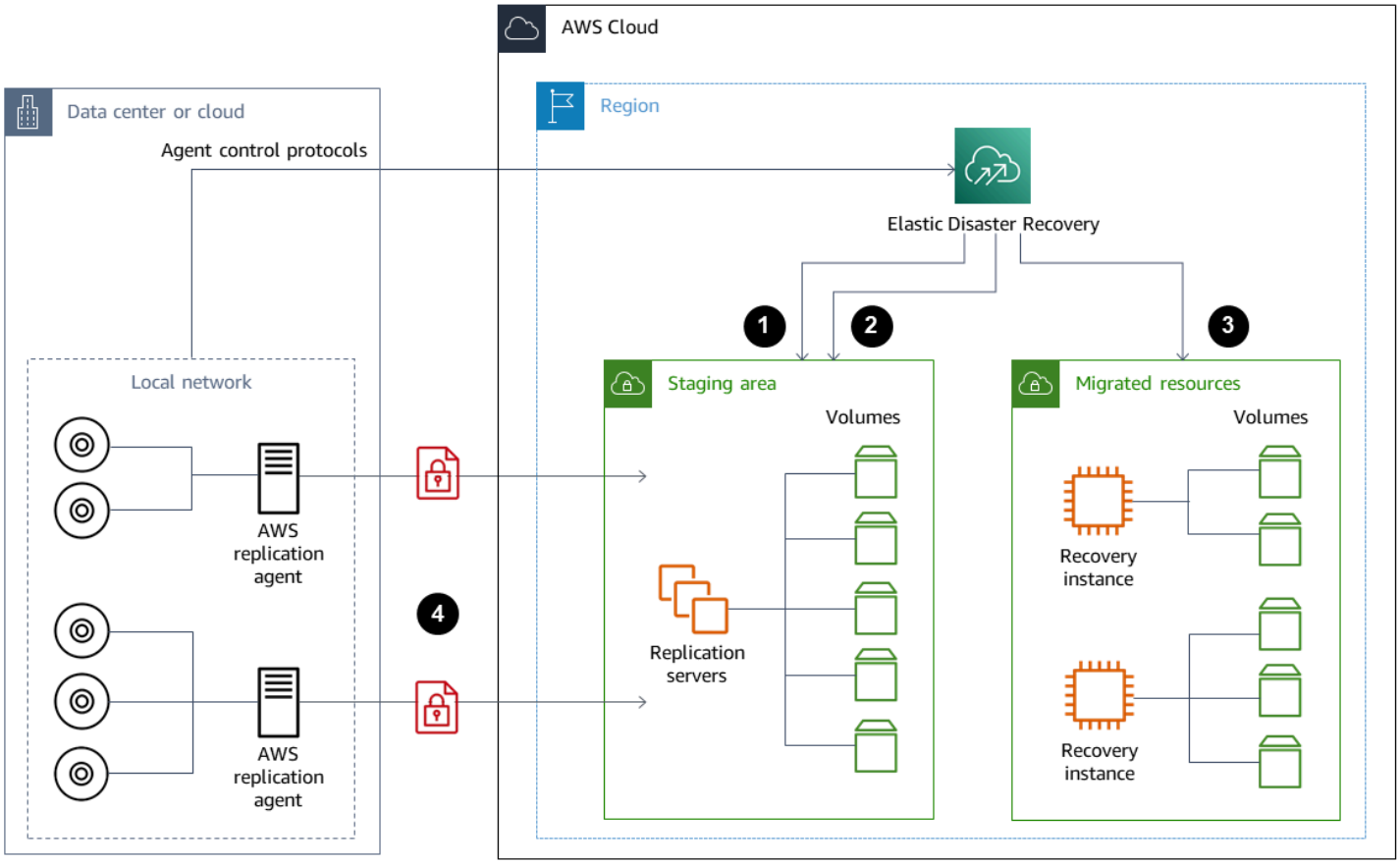
El uso AWS como entorno de recuperación ante desastres (DR) externo para cargas de trabajo locales es un escenario híbrido común. Defina sus objetivos de DR, incluidos los objetivos de tiempo y punto de recuperación necesarios, antes de seleccionar las tecnologías que va a utilizar. Para ayudarle con esta definición, puede usar la lista de verificación del plan de recuperación de desastres.

Hay varias opciones disponibles para ayudarle a configurar y aprovisionar rápidamente un entorno de DR en AWS. Asegúrese de tener en cuenta todas las dependencias de la carga de trabajo y pruebe su plan y solución de recuperación de desastres minuciosa y periódicamente para comprobar su integridad.

AWS permite AWS Elastic Disaster Recoverycrear una réplica completa de los servidores locales, incluidos el volumen raíz y el sistema operativo. AWS La recuperación de desastres elástica replica sus máquinas de forma continua en un área de almacenamiento de bajo costo en su cuenta de AWS de destino o Región de AWS preferida. La replicación a nivel de bloques es una réplica exacta del almacenamiento de sus servidores, que incluye el sistema operativo, la configuración del estado del sistema, las bases de datos, las aplicaciones y los archivos. Si se produce un desastre, puede indicarle a la recuperación de desastres elástica que lance rápidamente miles de máquinas en el estado totalmente aprovisionado en cuestión de minutos.

La recuperación de desastres elástica utiliza un agente instalado en cada uno de sus servidores en las instalaciones. Los agentes sincronizan el estado de sus servidores en las instalaciones

con los equivalentes de Amazon EC2 de menor potencia que se ejecutan en AWS. También puede automatizar su proceso de conmutación por error y conmutación por recuperación con la recuperación de desastres elástica. La automatización del proceso de conmutación por error y conmutación por recuperación puede ayudarle a alcanzar un objetivo de tiempo de recuperación (RTO) más bajo y más consistente.



1. Informes de estado del servidor de replicación
2. Recursos de la zona de puesta a disposición creados y terminados automáticamente
3. Instancias de recuperación lanzadas con un RTO de minutos y un RPO de segundos
4. Replicación continua a nivel de bloque (comprimida y cifrada)

Es importante probar el proceso de recuperación de desastres y comprobar que el entorno de ensayo activo no cree conflictos con el entorno en las instalaciones. Por ejemplo, confirme que las licencias apropiadas están disponibles y funcionando en su entorno en las instalaciones, de puesta en escena e iniciado de DR. Confirme también que cualquier proceso de tipo trabajador que pueda sondear y extraer trabajo de una base de datos central esté configurado adecuadamente para evitar superposiciones o conflictos. En el proceso de recuperación de desastres, incluya todos los

pasos necesarios que deban realizarse antes de que las instancias del servidor de recuperación entren en funcionamiento. Incluya también los pasos que debe seguir una vez que las instancias del servidor de recuperación estén en línea y disponibles. Puede utilizar soluciones como la Solución de Automatización de planes de AWS Elastic Disaster Recovery u otro enfoque que le ayude a automatizar sus planes de recuperación de desastres.

Puede usar una puerta de enlace de volumen de Storage Gateway para proporcionar volúmenes basados en la nube a sus servidores en las instalaciones. Estos volúmenes también se pueden aprovisionar rápidamente para su uso con Amazon EC2 mediante instantáneas de Amazon EBS. En concreto, las puertas de enlace de volumen almacenado proporcionan aplicaciones en las instalaciones con acceso de baja latencia a conjuntos de datos completos. Las puertas de enlace de volumen también proporcionan copias de seguridad duraderas basadas en instantáneas que se pueden restaurar para su uso en las instalaciones o para su uso con Amazon EC2. Puede programar las point-in-time instantáneas en función del objetivo del punto de recuperación (RPO) de su carga de trabajo.

> **Important**
>
> Los volúmenes de la puerta de enlace de volumen están diseñados para usarse como volúmenes de datos y no como volúmenes de arranque.

Puede utilizar una Imagen de máquina de Amazon (AMI) de Amazon EC2 con una configuración que se adapte a sus servidores en las instalaciones y especifique los volúmenes de datos por separado. Tras configurar y probar la AMI, aprovisione las instancias EC2 de la AMI junto con los volúmenes de datos en función de las instantáneas de la puerta de enlace de volumen. Este enfoque requiere que pruebe minuciosamente el entorno para comprobar que la instancia EC2 funciona correctamente, especialmente en el caso de las cargas de trabajo de Windows.

DR para cargas de trabajo nativas en la nube

Considere cómo se alinean sus cargas de trabajo nativas de la nube con sus objetivos de recuperación ante desastres. AWS ofrece múltiples zonas de disponibilidad en regiones de todo el mundo. Muchas empresas que utilizan la nube de AWS alinean sus arquitecturas de carga de trabajo y sus objetivos de recuperación de desastres para soportar la pérdida de una zona de disponibilidad. El pilar de la confiabilidad en el marco de AWS Well-Architected apoya esta mejor práctica. Puede diseñar sus cargas de trabajo y sus dependencias de servicios y aplicaciones para que usen varias

zonas de disponibilidad. A continuación, puede automatizar su DR y alcanzar sus objetivos de DR con una intervención mínima o nula.

Sin embargo, en la práctica, es posible que no pueda establecer una arquitectura redundante, activa y automatizada para todos sus componentes. Examine cada capa de su arquitectura para determinar los procesos de recuperación de desastres necesarios para alcanzar sus objetivos. Esto puede variar de una carga de trabajo a otra, con diferentes requisitos de arquitectura y servicio. Esta guía describe las consideraciones y opciones de Amazon EC2. Para otros servicios de AWS , puede consultar la documentación de AWS para determinar las opciones de alta disponibilidad y DR.

DR de Amazon EC2 en una sola zona de disponibilidad

Intente diseñar sus cargas de trabajo para brindar soporte y servicio de manera activa a los clientes de varias zonas de disponibilidad. Puede utilizar Amazon EC2 Auto Scaling y el equilibrador de carga elástico para lograr una arquitectura de servidor multi-AZ de Amazon EC2 y otros servicios.

Si su arquitectura tiene instancias EC2 que no pueden utilizar un equilibrador de carga y solo pueden ejecutar una sola instancia en un momento dado, puede usar cualquiera de las siguientes opciones.

- Cree un grupo de escalado automático que tenga un tamaño mínimo, máximo y deseado de 1 y esté configurado para varias zonas de disponibilidad. Cree una AMI que se pueda usar para reemplazar la instancia en caso de que falle. Asegúrese de definir la automatización y la configuración adecuadas para que una instancia recién aprovisionada desde la AMI se pueda configurar automáticamente y prestar servicio. Cree un equilibrador de carga que apunte al grupo de escalado automático y esté configurado para múltiples zonas de disponibilidad. Si lo desea, cree un alias de Amazon Route 53 que apunte al punto de conexión del equilibrador de carga.
- Cree un registro de Route 53 para la instancia activa y haga que sus clientes se conecten mediante este registro. Cree un script que cree una nueva AMI de la instancia activa y utilice la AMI para aprovisionar una nueva instancia de EC2 detenida en una zona de disponibilidad independiente. Configure el script para que se ejecute periódicamente y finalice la instancia detenida anterior. Si se produce un error en la zona de disponibilidad, inicie la instancia de respaldo en la zona de disponibilidad alternativa. A continuación, actualice el registro de Route 53 para que apunte a esta nueva instancia.

Pruebe su solución minuciosamente simulando el error contra el que se diseñó la solución. Tenga en cuenta también las actualizaciones que necesitará su solución de recuperación de desastres a medida que cambie la arquitectura de la carga de trabajo.

DR para Amazon EC2 en un fracaso regional

Los clientes con requisitos de disponibilidad muy altos (por ejemplo, aplicaciones de misión crítica que no toleran ningún tiempo de inactividad) pueden utilizarlos AWS en varias regiones para ofrecer una mayor resiliencia ante los problemas a nivel regional. Los clientes deben sopesar cuidadosamente la complejidad, el costo y el esfuerzo necesarios para establecer y mantener un plan de DR multirregional en comparación con las ventajas. AWS proporciona funciones que admiten arquitecturas multirregionales para la disponibilidad global, la conmutación por error y la recuperación ante desastres. Esta guía cubre algunas de las funciones disponibles que son específicas de la copia de seguridad y la recuperación para Amazon EC2.

AWS Las AMI y las instantáneas de Amazon EBS son recursos regionales que se pueden utilizar para aprovisionar nuevas instancias en una sola región. Sin embargo, puede copiar las instantáneas y las AMI a otra Región y utilizarlas para aprovisionar nuevas instancias en esa Región. Para respaldar un plan regional de recuperación ante fallos, puede automatizar el proceso de copiar las AMI y las instantáneas a otras regiones. AWS Backup y Amazon Data Lifecycle Manager admiten la copia entre regiones como parte de la configuración de backup.

AWS Elastic Disaster Recovery se puede utilizar para automatizar y replicar continuamente sus servidores Amazon EC2 de una región a una región de DR alternativa. La recuperación de desastres elástica puede simplificar su enfoque de DR multi-regional y ayudarle a probar periódicamente su plan de recuperación de desastres de Amazon EC2 entre regiones mediante simulacros. La recuperación de desastres elástica puede ayudarle cuando el copia de seguridad y la recuperación no pueden cumplir sus objetivos de RTO y RPO. La recuperación de desastres elástica puede ayudarle a reducir el RTO a minutos y el RPO a menos de un segundo.

Sea cual sea la solución que utilice, debe determinar el proceso de aprovisionamiento, conmutación por error y conmutación por recuperación que se utilizará en caso de una interrupción. Puede usar Route 53 con las comprobaciones de estado y la conmutación por error del sistema de nombres de dominio para respaldar su solución.

Eliminación de copias de seguridad

Para reducir los costos, limpie las copias de seguridad que ya no sean necesarias para fines de recuperación o retención. Puede utilizar AWS Backup y el Amazon Data Lifecycle Manager para automatizar la política de retención de una parte de las copias de seguridad. Sin embargo, incluso con estas herramientas implementadas, se necesita un enfoque de limpieza para las copias de seguridad que se realizan por separado.

Tener una estrategia de etiquetado es un requisito previo para realizar una estrategia de limpieza. Utilice el etiquetado para identificar los recursos que deben limpiarse, notificar a los propietarios de forma adecuada y automatizar el proceso de limpieza. Las copias de seguridad creadas por AWS tienen las fechas de creación alineadas con ellas, pero el etiquetado es importante para correlacionar las copias de seguridad con las cargas de trabajo, los requisitos de retención y la identificación de los puntos de restauración.

Puede implementar un proceso de limpieza de las instantáneas mediante la automatización. Por ejemplo, puede escanear su cuenta en busca de instantáneas y determinar si los volúmenes correspondientes están conectados o disponibles. Puede filtrar aún más los resultados según el límite de tiempo que especifique. Con las etiquetas adjuntas al volumen, puede enviar automáticamente un correo electrónico a los propietarios de las instantáneas y advertirles de que se ha programado la eliminación de sus instantáneas. Esta corrección automática se puede implementar mediante reglas AWS Config, un script usando AWS CLI, o una función de Lambda usando el AWS SDK.

Systems Manager proporciona los documentos AWS-DeleteEBSVolumeSnapshots y AWS-DeleteSnapshot para ayudarle a iniciar y automatizar la limpieza de las instantáneas de Amazon EBS. También puede utilizar el AWS CLI y AWS SDK para automatizar la limpieza de otros AWS recursos, como las instantáneas de Amazon RDS.

Preguntas frecuentes de copia de seguridad y recuperación

¿Qué programa de copias de seguridad debo seleccionar?

Definir una frecuencia de programación de copias de seguridad que se ajuste a su objetivo de punto de recuperación (RPO). Defina un tiempo de copia de seguridad en el que su carga de trabajo esté por debajo de la cantidad mínima de carga y en el que se pueda reducir el impacto en los usuarios. Cree una instantánea de un momento dado siempre que vaya a realizar un cambio significativo en su carga de trabajo.

¿Tengo que crear copias de seguridad en mis cuentas de desarrollo?

Pruebe los posibles cambios importantes en sus cuentas de desarrollo para sus cargas de trabajo y cree copias de seguridad antes de realizar cambios importantes. Es posible que tenga muchas más copias de seguridad de recuperación en un momento dado (PITR) en sus cuentas de desarrollo y de no producción derivadas de actividades de desarrollo y pruebas.

¿Puedo actualizar las aplicaciones y seguir utilizando un volumen de EBS mientras se crea una instantánea sin que tenga repercusiones?

Las instantáneas se realizan de una manera asíncrona, es decir, la instantánea de un momento dado se crea inmediatamente, pero su estado es pendiente hasta que todos los bloques modificados se han trasferido a Amazon S3. En el caso de instantáneas iniciales de gran tamaño o de instantáneas posteriores en las que se hayan modificado muchos bloques, la transferencia puede tardar varias horas. Mientras se está transferiendo, no le afectan las lecturas y escrituras continuas en el volumen. Para obtener más información, consulte la documentación del AWS.

Pasos siguientes

Comience por evaluar, implementar y probar su método de copias de seguridad y recuperación en un entorno que no sea de producción. Es importante probar minuciosamente el proceso de recuperación y validar que las cargas de trabajo restauradas funcionan según lo esperado.

Pruebe el proceso de restauración para un solo componente de su arquitectura, además de todos los componentes de su arquitectura. Valide el tiempo de recuperación de cada uno. Valide también el impacto de su proceso de copias de seguridad y restauración en dependencias ascendentes y descendentes. Confirme el impacto de cualquier interrupción del servicio en sus dependencias ascendentes y confirme el impacto descendente en sus copias de seguridad.

Recursos adicionales de

Recursos de AWS

- AWS Guía prescriptiva
- Documentación de AWS
- Referencia general de AWS
- Glosario de AWS

Servicios de AWS

- AWS Backup
- Amazon CloudWatch
- CloudWatch Eventos de Amazon
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- IAM
- Amazon RDS
- Amazon S3
- Storage Gateway
- AWS Systems Manager

Otros recursos

- Copia de seguridad y recuperación con AWS Backup (solución)
- Recuperación de cargas de trabajo ante desastres en AWS: recuperación en la nube (documento técnico)
- Serie sobre recuperación de desastres (publicaciones del blog sobre arquitectura de AWS)
- Lista de verificación del plan de recuperación de desastres
- Enfoques de copia de seguridad y recuperación mediante AWS (documento técnico, archivado)

- Cómo empezar con AWS Backup
- AWS Marketplace: copia de seguridad y restauración

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
información actualizada	Guía actualizada en la sección Amazon S3.	28 de junio de 2024
información actualizada	Información actualizada en la sección DR a AWS en las instalaciones.	13 de abril de 2023
Se agregó una sección	Se agregaron instrucciones y pasos para crear o restaurar una instancia a partir de una instantánea.	7 de marzo de 2023
Se ha añadido información sobre la recuperación de desastres elástica y se han añadido aclaraciones	En las secciones Recuperación ante desastres con protección de datos AWS y Selección de AWS servicios para la protección de datos, se agregó información sobre AWS Elastic Disaster Recovery. En las secciones Copias de seguridad y recuperación de Amazon EC2 con instantáneas y AMI, Preparación de un volumen EBS antes de crear una instantánea o una AMI y Restauración a partir de una instantánea de Amazon EBS o una AMI, se han añadido aclaraciones. Añadido a	19 de enero de 2023

	las Preguntas frecuentes sobre copia de seguridad y recuperación.	
Se ha añadido un enlace	Se ha añadido un enlace a la documentación de Administrador de ciclo de vida de datos de Amazon en la sección Administrador de ciclo de vida de datos de Amazon.	31 de octubre de 2022
información actualizada	Se actualizó la información sobre la restauración de volúmenes.	30 de agosto de 2022

Se ha actualizado la información y se ha añadido una nueva sección	En la sección Selección de AWS servicios para la protección de datos, se agregaron servicios. Añadida la sección Copia de seguridad y recuperación con AWS Backup. En la sección Copia de seguridad y recuperación mediante Amazon S3 y Amazon S3 Glacier, se ha añadido información sobre las nuevas clases de almacenamiento de Amazon S3 Glacier. En la sección Copia de seguridad y recuperación para Amazon EC2 con volúmenes EBS, se han añadido enlaces a documentación e información adicional. En la sección Backup and recovery of cloud native AWS services, se agregó una recomendación de uso AWS Backup. Se agregaron recursos en la sección Recursos adicionales.	28 de enero de 2022

información actualizada	Se agregó información sobre la configuración de las clases de almacenamiento a la sección Recuperación flexible de S3 Glacier. Se agregó información sobre la recuperación de instantán eas a la sección de Copias de seguridad y recuperación de Amazon EC2 con instantáneas y AMI.	9 de septiembre de 2021
información actualizada	En la AWS Backupsección, se agregó información sobre los AWS servicios AWS Backup compatibles.	1 de junio de 2021
Publicación inicial	—	29 de julio de 2020

AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por AWS Prescriptive Guidance. Para sugerir entradas, utilice el enlace Enviar comentarios al final del glosario.

Números

Las 7 R

Siete estrategias de migración comunes para trasladar aplicaciones a la nube. Estas estrategias se basan en las 5 R que Gartner identificó en 2011 y consisten en lo siguiente:

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: migre su base de datos Oracle local a la edición compatible con PostgreSQL de Amazon Aurora.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Amazon Relational Database Service (Amazon RDS) para Oracle en el. Nube de AWS
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Oracle en una instancia EC2 del. Nube de AWS
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

- Retirar: retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas (mediante una herramienta de replicación bidireccional o mediante operaciones de escritura doble) y ambas bases de datos gestionan las transacciones de las aplicaciones conectadas durante la migración. Este método permite la migración en lotes pequeños y controlados, en lugar de requerir una transición única. Es más flexible, pero requiere más trabajo que la migración activa-pasiva.

migración activa-pasiva

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas, pero solo la base de datos de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la base de datos de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función agregada

Función SQL que opera en un grupo de filas y calcula un único valor de retorno para el grupo. Entre los ejemplos de funciones agregadas se incluyen `SUM` y `MAX`.

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

antipatrones

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

control de aplicaciones

Un enfoque de seguridad que permite el uso únicamente de aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para el proceso de detección y análisis de la cartera y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte ¿Qué es la inteligencia artificial?

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo se utiliza AIOps en la estrategia de migración de AWS , consulte la Guía de integración de operaciones.

cifrado asimétrico

Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

atomicidad, consistencia, aislamiento, durabilidad (ACID)

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

control de acceso basado en atributos (ABAC)

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 AWS en la documentación AWS Identity and Access Management (IAM).

origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

Zona de disponibilidad

Una ubicación distinta dentro de una Región de AWS que está aislada de los fallos en otras zonas de disponibilidad y que proporciona una conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

AWS Marco de adopción de la nube (AWS CAF)

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de ayudar a preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la Página web de AWS CAF y el Documento técnico de AWS CAF.

AWS Marco de calificación de la carga de trabajo (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS

Schema Conversion Tool ().AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

Un bot malo

Un bot destinado a interrumpir o causar daño a personas u organizaciones.

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las llamadas sospechosas a la API y acciones similares. Para obtener más información, consulte Datos en un gráfico de comportamiento en la documentación de Detective.

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también endianness.

clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

implementación azul/verde

Una estrategia de despliegue en la que se crean dos entornos separados pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación en el otro entorno (verde). Esta estrategia le ayuda a revertirla rápidamente con un impacto mínimo.

bot

Una aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan información en Internet. Algunos otros bots, conocidos como bots malos, tienen como objetivo interrumpir o causar daños a personas u organizaciones.

botnet

Redes de bots que están infectadas por malware y que están bajo el control de una sola parte, conocida como pastor u operador de bots. Las botnets son el mecanismo más conocido para escalar los bots y su impacto.

rama

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte Acerca de las sucursales (GitHub documentación).

acceso con cristales rotos

En circunstancias excepcionales y mediante un proceso aprobado, un usuario puede acceder rápidamente a un sitio para el Cuenta de AWS que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador Implemente procedimientos de rotura de cristales en la guía Well-Architected AWS .

estrategia de implementación sobre infraestructura existente

La infraestructura existente en su entorno. Al adoptar una estrategia de implementación sobre infraestructura existente para una arquitectura de sistemas, se diseña la arquitectura en función de las limitaciones de los sistemas y la infraestructura actuales. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

caché de búfer

El área de memoria donde se almacenan los datos a los que se accede con más frecuencia.

capacidad empresarial

Lo que hace una empresa para generar valor (por ejemplo, ventas, servicio al cliente o marketing). Las arquitecturas de microservicios y las decisiones de desarrollo pueden estar impulsadas por las capacidades empresariales. Para obtener más información, consulte la sección Organizado en torno a las capacidades empresariales del documento técnico Ejecutar microservicios en contenedores en AWS.

planificación de la continuidad del negocio (BCP)

Plan que aborda el posible impacto de un evento disruptivo, como una migración a gran escala en las operaciones y permite a la empresa reanudar las operaciones rápidamente.

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

El lanzamiento lento e incremental de una versión para los usuarios finales. Cuando se tiene confianza, se despliega la nueva versión y se reemplaza la versión actual en su totalidad.

CCoE

Consulte el Centro de excelencia en la nube.

CDC

Consulte la captura de datos de cambios.

captura de datos de cambio (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Puede utilizar los CDC para diversos fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

ingeniería del caos

Introducir intencionalmente fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

cifrado del cliente

Cifrado de datos localmente, antes de que el objetivo los Servicio de AWS reciba.

Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las publicaciones de CCoE en el blog de estrategia Nube de AWS empresarial.

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar conectada a la tecnología de computación perimetral.

modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte Creación de su modelo operativo de nube.

etapas de adopción de la nube

Las cuatro fases por las que suelen pasar las organizaciones cuando migran a Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realización de inversiones fundamentales para escalar la adopción de la nube (p. ej., crear una zona de aterrizaje, definir un CCoE, establecer un modelo de operaciones)
- Migración: migración de aplicaciones individuales

- Reinvención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la entrada del blog The Journey Toward Cloud-First & the Stages of Adoption del blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Los repositorios en la nube más comunes incluyen GitHub o AWS CodeCommit. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola canalización de CI/CD puede utilizar varios repositorios.

caché en frío

Una caché de búfer que está vacía no está bien poblada o contiene datos obsoletos o irrelevantes. Esto afecta al rendimiento, ya que la instancia de la base de datos debe leer desde la memoria principal o el disco, lo que es más lento que leer desde la memoria caché del búfer.

datos fríos

Datos a los que se accede con poca frecuencia y que suelen ser históricos. Al consultar este tipo de datos, normalmente se aceptan consultas lentas. Trasladar estos datos a niveles o clases de almacenamiento de menor rendimiento y menos costosos puede reducir los costos.

visión artificial (CV)

Campo de la IA que utiliza el aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, AWS Panorama ofrece dispositivos que añaden CV a las redes de cámaras locales, y Amazon SageMaker proporciona algoritmos de procesamiento de imágenes para CV.

desviación de configuración

En el caso de una carga de trabajo, un cambio de configuración con respecto al estado esperado. Puede provocar que la carga de trabajo deje de cumplir las normas y, por lo general, es gradual e involuntario.

base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los datos de una CMDB se utilizan en la etapa de detección y análisis de la cartera de productos durante la migración.

paquete de conformidad

Conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus comprobaciones de conformidad y seguridad. Puede implementar un paquete de conformidad como una entidad única en una región Cuenta de AWS y, o en una organización, mediante una plantilla YAML. Para obtener más información, consulta los paquetes de conformidad en la documentación. AWS Config

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, presentación y producción del proceso de lanzamiento del software. La CI/CD se describe comúnmente como una canalización. La CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Consulte visión artificial.

D

datos en reposo

Datos que están estacionarios en la red, como los datos que se encuentran almacenados.

clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad del AWS Well-Architected Framework. Para obtener más información, consulte Clasificación de datos.

desviación de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada a lo largo del tiempo. La desviación de los datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

datos en tránsito

Datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red.

malla de datos

Un marco arquitectónico que proporciona una propiedad de datos distribuida y descentralizada con administración y gobierno centralizados.

minimización de datos

El principio de recopilar y procesar solo los datos estrictamente necesarios. Practicar la minimización de los datos Nube de AWS puede reducir los riesgos de privacidad, los costos y la huella de carbono de la analítica.

perímetro de datos

Un conjunto de barreras preventivas en su AWS entorno que ayudan a garantizar que solo las identidades confiables accedan a los recursos confiables desde las redes esperadas. Para obtener más información, consulte Crear un perímetro de datos sobre. AWS

preprocesamiento de datos

Transformar los datos sin procesar en un formato que su modelo de ML pueda analizar fácilmente. El preprocesamiento de datos puede implicar eliminar determinadas columnas o filas y corregir los valores faltantes, incoherentes o duplicados.

procedencia de los datos

El proceso de rastrear el origen y el historial de los datos a lo largo de su ciclo de vida, por ejemplo, la forma en que se generaron, transmitieron y almacenaron los datos.

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

Un sistema de administración de datos que respalde la inteligencia empresarial, como el análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para consultas y análisis.

lenguaje de definición de datos (DDL)

Instrucciones o comandos para crear o modificar la estructura de tablas y objetos de una base de datos.

lenguaje de manipulación de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

defense-in-depth

Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la integridad y la disponibilidad de la red y de los datos que contiene. Al adoptar esta estrategia AWS, se añaden varios controles en diferentes capas de la AWS Organizations estructura para ayudar a proteger los recursos. Por ejemplo, un defense-in-depth enfoque podría combinar la autenticación multifactorial, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta

cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations .

Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

entorno de desarrollo

Consulte entorno.

control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte Controles de detección en Implementación de controles de seguridad en AWS.

asignación de flujos de valor para el desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSM amplía el proceso de asignación del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

tabla de dimensiones

En un esquema en estrella, tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos de una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se utilizan habitualmente para restringir consultas, filtrar y etiquetar conjuntos de resultados.

desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

recuperación de desastres (DR)

La estrategia y el proceso que se utilizan para minimizar el tiempo de inactividad y la pérdida de datos ocasionados por un desastre. Para obtener más información, consulte Recuperación ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Este concepto lo introdujo Eric Evans en su libro, Diseño impulsado por el dominio: abordando la complejidad en el corazón del software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración de referencia. Por ejemplo, puedes usarlo AWS CloudFormation para detectar desviaciones en los recursos del sistema o puedes usarlo AWS Control Tower para detectar cambios en tu landing zone que puedan afectar al cumplimiento de los requisitos de gobierno.

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

computación en la periferia

La tecnología que aumenta la potencia de cálculo de los dispositivos inteligentes en la periferia de una red de IoT. En comparación con la computación en nube, la computación perimetral puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

cifrado

Proceso informático que transforma datos de texto plano, legibles por humanos, en texto cifrado.

clave de cifrado

Cadena criptográfica de bits aleatorios que se genera mediante un algoritmo de cifrado. Las claves pueden variar en longitud y cada una se ha diseñado para ser impredecible y única.

endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian almacenan primero el byte menos significativo.

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto final AWS PrivateLink y conceder permisos a otros directores Cuentas de AWS o a AWS Identity and Access Management (IAM). Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte Creación de un servicio de punto de conexión en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

planificación de recursos empresariales (ERP)

Un sistema que automatiza y gestiona los procesos empresariales clave (como la contabilidad, el MES y la gestión de proyectos) de una empresa.

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte el cifrado de sobres en la documentación de AWS Key Management Service (AWS KMS).

environment

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.
- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En una canalización de CI/CD, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas AWS de seguridad de CAF incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

PERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para

encontrar patrones, detectar anomalías y comprobar las suposiciones. El EDA se realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

F

tabla de datos

La tabla central de un esquema en forma de estrella. Almacena datos cuantitativos sobre las operaciones comerciales. Normalmente, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

fallan rápidamente

Una filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de un enfoque ágil.

límite de aislamiento de fallas

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para obtener más información, consulte Límites de AWS aislamiento de errores.

rama de característica

Consulte la sucursal.

características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, esto se expresa como una puntuación numérica que se puede calcular mediante diversas técnicas, como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con:AWS.

transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

FGAC

Consulte el control de acceso detallado.

control de acceso preciso (FGAC)

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.

migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la captura de datos modificados para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

G

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

En Amazon CloudFront, una opción para impedir que los usuarios de países específicos accedan a las distribuciones de contenido. Puede utilizar una lista de permitidos o bloqueados para especificar los países aprobados y prohibidos. Para obtener más información, consulta Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, y el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como implementación sobre infraestructura existente. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y la conformidad en todas las unidades organizativas (OU). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de permisos de IAM. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

JA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que utilice un motor de base de datos diferente (por ejemplo, de Oracle a Amazon Aurora). La migración heterogénea suele ser parte de un esfuerzo de rediseño de la arquitectura y convertir el esquema puede ser una tarea compleja. AWS ofrece AWS SCT, lo cual ayuda con las conversiones de esquemas.

alta disponibilidad (HA)

La capacidad de una carga de trabajo para funcionar de forma continua, sin intervención, en caso de desafíos o desastres. Los sistemas de alta disponibilidad están diseñados para realizar una conmutación por error automática, ofrecer un rendimiento de alta calidad de forma constante y gestionar diferentes cargas y fallos con un impacto mínimo en el rendimiento.

modernización histórica

Un enfoque utilizado para modernizar y actualizar los sistemas de tecnología operativa (TO) a fin de satisfacer mejor las necesidades de la industria manufacturera. Un histórico es un tipo de base de datos que se utiliza para recopilar y almacenar datos de diversas fuentes en una fábrica.

migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS para SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, las revisiones suelen realizarse fuera del flujo de trabajo habitual de las DevOps versiones.

periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

I

IaC

Vea la infraestructura como código.

políticas basadas en identidad

Política asociada a uno o más directores de IAM que define sus permisos en el Nube de AWS entorno.

aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, parchear o modificar la infraestructura existente. Las infraestructuras inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las prácticas recomendadas para implementar con una infraestructura inmutable en Well-Architected Framework AWS .

VPC entrante (de entrada)

En una arquitectura de AWS cuentas múltiples, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

Industria 4.0

Un término que Klaus Schwab introdujo en 2016 para referirse a la modernización de los procesos de fabricación mediante avances en la conectividad, los datos en tiempo real, la automatización, el análisis y la inteligencia artificial/aprendizaje automático.

infraestructura

Todos los recursos y activos que se encuentran en el entorno de una aplicación.

infraestructura como código (IaC)

Proceso de aprovisionamiento y administración de la infraestructura de una aplicación mediante un conjunto de archivos de configuración. La IaC se ha diseñado para ayudarlo a centralizar la administración de la infraestructura, estandarizar los recursos y escalar con rapidez a fin de que los entornos nuevos sean repetibles, fiables y consistentes.

Internet de las cosas industrial (IIoT)

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte Creación de una estrategia de transformación digital del Internet de las cosas industrial (IIoT).

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red entre las VPC (iguales o Regiones de AWS diferentes), Internet y las redes locales. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte ¿Qué es IoT?.

interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para más información, consulte Interpretabilidad del modelo de machine learning con AWS.

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. La ITIL proporciona la base para la ITSM.

administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con las herramientas de ITSM, consulte la Guía de integración de operaciones.

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

zona de aterrizaje

Una landing zone es un AWS entorno multicuenta bien diseñado, escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte Configuración de un entorno de AWS seguro y escalable con varias cuentas.

migración grande

Migración de 300 servidores o más.

LBAC

Consulte el control de acceso basado en etiquetas.

privilegio mínimo

La práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Aplicar permisos de privilegio mínimo en la documentación de IAM.

migrar mediante lift-and-shift

Ver 7 Rs.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Véase también endianness.

entornos inferiores

Véase entorno.

M

machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte Machine learning.

rama principal

Ver sucursal.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware puede interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los registradores de pulsaciones de teclas.

servicios gestionados

Servicios de AWS para los que AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y usted accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios gestionados. También se conocen como servicios abstractos.

sistema de ejecución de fabricación (MES)

Un sistema de software para rastrear, monitorear, documentar y controlar los procesos de producción que convierten las materias primas en productos terminados en el taller.

MAP

Consulte Migration Acceleration Program.

mecanismo

Un proceso completo en el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para realizar ajustes. Un mecanismo es un ciclo que se refuerza y mejora a sí mismo a medida que funciona. Para obtener más información, consulte Creación de mecanismos en el AWS Well-Architected Framework.

cuenta de miembro

Todas las Cuentas de AWS demás cuentas, excepto la de administración, que forman parte de una organización. AWS Organizations Una cuenta no puede pertenecer a más de una organización a la vez.

MES

Consulte el sistema de ejecución de la fabricación.

Transporte telemétrico de Message Queue Queue (MQTT)

Un protocolo de comunicación ligero machine-to-machine (M2M), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.

microservicio

Un servicio pequeño e independiente que se comunica a través de API bien definidas y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo, un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte Integrar microservicios mediante servicios sin servidor. AWS

arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante API ligeras. Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte Implementación de microservicios en. AWS

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la estrategia de migración de AWS.

fábrica de migración

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen incluir a analistas y propietarios de operaciones, empresas, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan a pasos agigantados. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la discusión sobre las fábricas de migración y la Guía de fábricas de migración a la nube en este contenido.

metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son la subred de destino, el grupo de seguridad y AWS la cuenta.

patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: rehospede la migración a Amazon EC2 AWS con Application Migration Service.

Migration Portfolio Assessment (MPA)

Una herramienta en línea que proporciona información para validar el modelo de negocio para migrar a. Nube de AWS La MPA ofrece una evaluación detallada de la cartera (adecuación del

tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar sus puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas mediante el AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. La MRA es la primera fase de la estrategia de migración de AWS.

estrategia de migración

El enfoque utilizado para migrar una carga de trabajo a. Nube de AWS Para obtener más información, consulte la entrada de las 7 R de este glosario y consulte Movilice a su organización para acelerar las migraciones a gran escala.

ML

Consulte el aprendizaje automático.

modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia y aprovechar las innovaciones. Para obtener más información, consulte Estrategia para modernizar las aplicaciones en el Nube de AWS.

evaluación de la preparación para la modernización

Evaluación que ayuda a determinar la preparación para la modernización de las aplicaciones de una organización; identifica los beneficios, los riesgos y las dependencias; y determina qué tan bien la organización puede soportar el estado futuro de esas aplicaciones. El resultado de la evaluación es un esquema de la arquitectura objetivo, una hoja de ruta que detalla las fases de desarrollo y los hitos del proceso de modernización y un plan de acción para abordar las brechas identificadas. Para obtener más información, consulte Evaluación de la preparación para la modernización de las aplicaciones en el Nube de AWS.

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la

aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MAPA

Consulte la evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

Un proceso que ayuda a generar predicciones para varias clases (predice uno de más de dos resultados). Por ejemplo, un modelo de ML podría preguntar "¿Este producto es un libro, un automóvil o un teléfono?" o "¿Qué categoría de productos es más interesante para este cliente?".

infraestructura mutable

Un modelo que actualiza y modifica la infraestructura existente para las cargas de trabajo de producción. Para mejorar la coherencia, la fiabilidad y la previsibilidad, el AWS Well-Architected Framework recomienda el uso de una infraestructura inmutable como práctica recomendada.

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

Método de migración en el que la carga de trabajo de origen se elimina durante el proceso de migración. Este método implica un tiempo de inactividad prolongado y, por lo general, se utiliza para cargas de trabajo pequeñas y no críticas.

OI

Consulte integración de operaciones.

OLA

Véase el acuerdo a nivel operativo.

migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

Comunicaciones de proceso abierto: arquitectura unificada (OPC-UA)

Un protocolo de comunicación machine-to-machine (M2M) para la automatización industrial. El OPC-UA proporciona un estándar de interoperabilidad con esquemas de cifrado, autenticación y autorización de datos.

acuerdo de nivel operativo (OLA)

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse entre sí, para respaldar un acuerdo de nivel de servicio (SLA).

revisión de la preparación operativa (ORR)

Una lista de preguntas y las mejores prácticas asociadas que le ayudan a comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles fallos. Para obtener más información, consulte Operational Readiness Reviews (ORR) en AWS Well-Architected Framework.

tecnología operativa (OT)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En la industria manufacturera, la integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

Proceso de modernización de las operaciones en la nube, que implica la planificación de la preparación, la automatización y la integración. Para obtener más información, consulte la Guía de integración de las operaciones.

registro de seguimiento organizativo

Un registro creado por el AWS CloudTrail que se registran todos los eventos para todos Cuentas de AWS los miembros de una organización AWS Organizations. Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte Crear un registro para una organización en la CloudTrail documentación.

administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. La OCM ayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de personal, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la Guía de OCM.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas al bucket de S3.

identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando utiliza OAI, CloudFront crea un principal con el que Amazon S3 puede autenticarse. Los directores autenticados solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica. CloudFront Consulte también el OAC, que proporciona un control de acceso más detallado y mejorado.

O

Consulte la revisión de la preparación operativa.

NO

Consulte tecnología operativa.

VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

P

límite de permisos

Una política de administración de IAM que se adjunta a las entidades principales de IAM para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte Límites de permisos en la documentación de IAM.

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos de información de identificación personal son los nombres, las direcciones y la información de contacto.

PII

Consulte la información de identificación personal.

manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

política

Un objeto que puede definir los permisos (consulte la política basada en la identidad), especifique las condiciones de acceso (consulte la política basada en los recursos) o defina los permisos máximos para todas las cuentas de una organización AWS Organizations (consulte la política de control de servicios).

persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades. Para obtener más información, consulte Habilitación de la persistencia de datos en los microservicios.

evaluación de cartera

Proceso de detección, análisis y priorización de la cartera de aplicaciones para planificar la migración. Para obtener más información, consulte la Evaluación de la preparación para la migración.

predicate

Una condición de consulta que devuelve `true` o`false`, por lo general, se encuentra en una cláusula. `WHERE`

pulsar un predicado

Técnica de optimización de consultas de bases de datos que filtra los datos de la consulta antes de transferirlos. Esto reduce la cantidad de datos que se deben recuperar y procesar de la base de datos relacional y mejora el rendimiento de las consultas.

control preventivo

Un control de seguridad diseñado para evitar que ocurra un evento. Estos controles son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Para obtener más información, consulte Controles preventivos en Implementación de controles de seguridad en AWS.

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz para un Cuenta de AWS rol de IAM o un usuario. Para obtener más información, consulte Entidad principal en Términos y conceptos de roles en la documentación de IAM.

Privacidad desde el diseño

Un enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de ingeniería.

zonas alojadas privadas

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. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Un control de seguridad diseñado para evitar el despliegue de recursos no conformes. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en Implementación de controles de seguridad en AWS.

gestión del ciclo de vida del producto (PLM)

La gestión de los datos y los procesos de un producto a lo largo de todo su ciclo de vida, desde el diseño, el desarrollo y el lanzamiento, pasando por el crecimiento y la madurez, hasta el rechazo y la retirada.

entorno de producción

Consulte el entorno.

controlador lógico programable (PLC)

En la fabricación, una computadora adaptable y altamente confiable que monitorea las máquinas y automatiza los procesos de fabricación.

seudonimización

El proceso de reemplazar los identificadores personales de un conjunto de datos por valores de marcadores de posición. La seudonimización puede ayudar a proteger la privacidad personal. Los datos seudonimizados siguen considerándose datos personales.

publicar/suscribirse (pub/sub)

Un patrón que permite las comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un MES basado en microservicios, un microservicio puede publicar mensajes de eventos en un canal al que se puedan suscribir otros microservicios. El sistema puede añadir nuevos microservicios sin cambiar el servicio de publicación.

Q

plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos relacional SQL.

regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas, restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

R

Matriz RACI

Véase responsable, responsable, consultado, informado (RACI).

ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

Matriz RASCI

Véase responsable, responsable, consultado, informado (RACI).

RCAC

Consulte control de acceso por filas y columnas.

read replica

Una copia de una base de datos que se utiliza con fines de solo lectura. Puede enrutar las consultas a la réplica de lectura para reducir la carga en la base de datos principal.

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo 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.

objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio.

refactorizar

Ver 7 Rs.

Región

Una colección de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para obtener más información, consulte Regiones de AWS Especificar qué cuenta puede usar.

regresión

Una técnica de ML que predice un valor numérico. Por ejemplo, para resolver el problema de "¿A qué precio se venderá esta casa?", un modelo de ML podría utilizar un modelo de regresión lineal para predecir el precio de venta de una vivienda en función de datos conocidos sobre ella (por ejemplo, los metros cuadrados).

volver a alojar

Consulte 7 Rs.

versión

En un proceso de implementación, el acto de promover cambios en un entorno de producción.

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resilencia

La capacidad de una aplicación para resistir las interrupciones o recuperarse de ellas. La alta disponibilidad y la recuperación ante desastres son consideraciones comunes a la hora de planificar la resiliencia en el. Nube de AWS Para obtener más información, consulte Nube de AWS Resiliencia.

política basada en recursos

Una política asociada a un recurso, como un bucket de Amazon S3, un punto de conexión o una clave de cifrado. Este tipo de política especifica a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

matriz responsable, confiable, consultada e informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina matriz RASCI y, si la excluye, se denomina matriz RACI.

control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte Controles receptivos en Implementación de controles de seguridad en AWS.

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

rotación

Proceso de actualizar periódicamente un secreto para dificultar el acceso de un atacante a las credenciales.

control de acceso por filas y columnas (RCAC)

El uso de expresiones SQL básicas y flexibles que tienen reglas de acceso definidas. El RCAC consta de permisos de fila y máscaras de columnas.

RPO

Consulte el objetivo del punto de recuperación.

RTO

Consulte el objetivo de tiempo de recuperación.

manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

S

SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión AWS Management Console o llamar a las operaciones de la AWS API sin tener que crear un usuario en IAM para todos los miembros de la organización. Para obtener más información sobre la federación basada en SAML 2.0, consulte Acerca de la federación basada en SAML 2.0 en la documentación de IAM.

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener

más información, consulta ¿Qué hay en un secreto de Secrets Manager? en la documentación de Secrets Manager.

control de seguridad

Barrera de protección técnica o administrativa que impide, detecta o reduce la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Hay cuatro tipos principales de controles de seguridad: preventivos, de detección, de respuesta y proactivos.

refuerzo de la seguridad

Proceso de reducir la superficie expuesta a ataques para hacerla más resistente a los ataques. Esto puede incluir acciones, como la eliminación de los recursos que ya no se necesitan, la implementación de prácticas recomendadas de seguridad consistente en conceder privilegios mínimos o la desactivación de características innecesarias en los archivos de configuración.

sistema de información sobre seguridad y administración de eventos (SIEM)

Herramientas y servicios que combinan sistemas de administración de información sobre seguridad (SIM) y de administración de eventos de seguridad (SEM). Un sistema de SIEM recopila, monitorea y analiza los datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

automatización de la respuesta de seguridad

Una acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o remediarlo. Estas automatizaciones sirven como controles de seguridad detectables o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. Algunos ejemplos de acciones de respuesta automatizadas incluyen la modificación de un grupo de seguridad de VPC, la aplicación de parches a una instancia de Amazon EC2 o la rotación de credenciales.

cifrado del servidor

Cifrado de los datos en su destino, por parte de quien Servicio de AWS los recibe.

política de control de servicio (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. Las SCP definen barreras de protección o establecen límites a las acciones que un administrador puede delegar en los usuarios o roles. Puede utilizar las SCP como listas de permitidos o rechazados, para especificar qué servicios o acciones se encuentra permitidos o prohibidos. Para obtener más información, consulte las políticas de control de servicios en la AWS Organizations documentación.

punto de enlace de servicio

La URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte Puntos de conexión de Servicio de AWS en Referencia general de AWS.

acuerdo de nivel de servicio (SLA)

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

indicador de nivel de servicio (SLI)

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

objetivo de nivel de servicio (SLO)

Una métrica objetivo que representa el estado de un servicio, medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

Un modelo que describe la responsabilidad que compartes con respecto a la seguridad y AWS el cumplimiento de la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el Modelo de responsabilidad compartida.

SIEM

Consulte la información de seguridad y el sistema de gestión de eventos.

punto único de fallo (SPOF)

Una falla en un único componente crítico de una aplicación que puede interrumpir el sistema.

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

ASÍ QUE

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para obtener más información, consulte Enfoque gradual para modernizar las aplicaciones en el. Nube de AWS

SPOT

Consulte el punto único de falla.

esquema en forma de estrella

Estructura organizativa de una base de datos que utiliza una tabla de datos grande para almacenar datos transaccionales o medidos y una o más tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para usarse en un almacén de datos o con fines de inteligencia empresarial.

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado. Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue presentado por Martin Fowler como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

Un intervalo de direcciones IP en la VPC. Una subred debe residir en una sola zona de disponibilidad.

supervisión, control y adquisición de datos (SCADA)

En la industria manufacturera, un sistema que utiliza hardware y software para monitorear los activos físicos y las operaciones de producción.

cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

pruebas sintéticas

Probar un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o monitorear el rendimiento. Puede usar Amazon CloudWatch Synthetics para crear estas pruebas.

T

etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Para obtener más información, consulte Etiquetado de los recursos de AWS.

variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte entorno.

entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

puerta de enlace de tránsito

Centro de tránsito de red que puede utilizar para interconectar las VPC y las redes en las instalaciones. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración por usted. Para obtener más información, consulte AWS Organizations Utilización con otros AWS servicios en la AWS Organizations documentación.

ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

equipo de dos pizzas

Un DevOps equipo pequeño al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

U

incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos. Para más información, consulte la guía Cuantificación de la incertidumbre en los sistemas de aprendizaje profundo.

tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

entornos superiores

Ver entorno.

V

succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

Emparejamiento de VPC

Conexión entre dos VPC que permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte ¿Qué es una interconexión de VPC? en la documentación de Amazon VPC.

vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

W

caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

función de ventana

Función SQL que realiza un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para procesar tareas, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

GUSANO

Mira, escribe una vez, lee muchas.

WQF

Consulte el marco de calificación de cargas de trabajo de AWS.

escribe una vez, lee muchas (WORM)

Un modelo de almacenamiento que escribe los datos una sola vez y evita que los datos se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no pueden cambiarlos. Esta infraestructura de almacenamiento de datos se considera inmutable.

Z

ataque de día cero

Un ataque, normalmente de malware, que aprovecha una vulnerabilidad de día cero.

vulnerabilidad de día cero

Un defecto o una vulnerabilidad sin mitigación en un sistema de producción. Los agentes de amenazas pueden usar este tipo de vulnerabilidad para atacar el sistema. Los desarrolladores suelen darse cuenta de la vulnerabilidad a raíz del ataque.

aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

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.