aws

Diseño e implementación del registro y la supervisión con Amazon CloudWatch

AWS Guía prescriptiva

AWS Guía prescriptiva: Diseño e implementación del registro y la supervisión con Amazon CloudWatch

Table of Contents

Diseño e implementación del registro y la monitorización con Amazon CloudWatch

Khurram Nizami, Amazon Web Services (AWS)

Abril de 2023 (historial del documento)

Esta guía le ayuda a diseñar e implementar el registro y la supervisión con Amazon CloudWatch y los servicios de administración y gobierno relacionados de Amazon Web Services (AWS) para cargas de trabajo que utilizan instancias de Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) y servidores locales. AWS Lambda La guía está destinada a los equipos de operaciones, los DevOps ingenieros y los ingenieros de aplicaciones que gestionan las cargas de trabajo en laAWS nube.

Su enfoque de registro y monitoreo debe basarse en los seis pilares del marcoAWS Well-Architected. Estos pilares son la excelencia operativa, la seguridad, la confiabilidad, la eficiencia del rendimiento y la optimización de costos. Una solución de monitoreo y alarma bien diseñada mejora la confiabilidad y el rendimiento al ayudarlo a analizar y ajustar su infraestructura de manera proactiva.

En esta guía no se analiza exhaustivamente el registro y la monitorización para garantizar la seguridad o la optimización de costes, ya que se trata de temas que requieren una evaluación en profundidad. Hay muchosAWS servicios que admiten el registro y la supervisión de la seguridad AWS CloudTrailAWS Config, incluidos Amazon Inspector, Amazon Detective, Amazon Macie GuardDuty, Amazon y AWS Security Hub. También puede utilizar AWS Cost ExplorerAWSlos presupuestos y las métricasCloudWatch de facturación para optimizar los costos.

La siguiente tabla describe las seis áreas que debe abordar su solución de registro y monitoreo.

Capturar e incorporar métricas y archivos de registro	Identifique, configure y envíe registros y métricas del sistema y las aplicaciones aAWS servicios de diferentes fuentes.
Búsqueda y análisis de registros	Busque y analice los registros para la administración de operaciones, la identificación de problemas, la solución de problemas y el análisis de aplicaciones.

Monitorización de métricas y alarmas	Identifique las observaciones y tendencias de sus cargas de trabajo y actúe en función de ellas.
Supervisión de la disponibilidad de aplicaciones y servicios	Reduzca el tiempo de inactividad y mejore su capacidad de cumplir los objetivos de nivel de servicio mediante la supervisión continua de la disponibilidad del servicio.
Aplicaciones de rastreo	Realice un seguimiento de las solicitudes de aplicaciones en sistemas y dependencias externas para ajustar el rendimiento, analizar la causa raíz y solucionar problemas.
Creación de paneles y visualizaciones	Cree paneles que se centren en las métricas y observaciones relevantes para sus sistemas y cargas de trabajo, lo que ayuda a la mejora continua y al descubrimiento proactivo de los problemas.

CloudWatch puede cumplir con la mayoría de los requisitos de registro y monitoreo y proporciona una solución confiable, escalable y flexible. MuchosAWS servicios proporcionan CloudWatch métricas automáticamente, además de la integración de CloudWatch registros para el monitoreo y el análisis. CloudWatch también proporciona agentes y controladores de registro para admitir una variedad de opciones de procesamiento, como servidores (tanto en la nube como en las instalaciones), contenedores y computación sin servidor. Esta guía también incluye los siguientesAWS servicios que se utilizan para el registro y la supervisión:

- AWS Systems ManagerDistribuidor, Systems Manager, State Manager y Systems Manager Automation para automatizar, configurar y actualizar el CloudWatch agente para sus instancias de EC2 y servidores locales
- Amazon OpenSearch Service para agregación, búsqueda y análisis avanzados de registros
- Verificaciones de estado y pruebas CloudWatchSynthetics de Amazon Route 53 para monitorear la disponibilidad de aplicaciones y servicios
- Amazon Managed Prometheus Managed Service for a escala

- AWS X-Raypara el seguimiento de aplicaciones y el análisis del tiempo de ejecución
- Amazon gestionó Grafana para visualizar y analizar datos de múltiples fuentes (por ejemplo CloudWatch, Amazon OpenSearch Service y Amazon Timestream)

Los serviciosAWS informáticos que elija también afectan a la implementación y la configuración de la solución de registro y monitoreo. Por ejemplo, CloudWatch la implementación y la configuración son diferentes para Amazon EC2, Amazon ECS, Amazon EKS y Lambda.

Los propietarios de aplicaciones y cargas de trabajo a menudo pueden olvidarse del registro y la supervisión o configurarlos e implementarlos de manera incoherente. Esto significa que las cargas de trabajo entran en producción con una observabilidad limitada, lo que provoca retrasos en la identificación de los problemas y aumenta el tiempo necesario para solucionarlos. Como mínimo, la solución de registro y monitoreo debe abordar la capa de sistemas para los registros y métricas a nivel del sistema operativo (SO), además de la capa de aplicación para los registros y métricas de las aplicaciones. La guía proporciona un enfoque recomendado para abordar estas dos capas en diferentes tipos de procesamiento, incluidos los tres tipos de procesamiento que se describen en la siguiente tabla.

Instancias de EC2 inmutables y de larga ejecución	Registros y métricas de sistemas y aplicaciones en varios sistemas operativos (OS) en variasAWS regiones o cuentas.
Contenedores	Registros y métricas de sistemas y aplicaciones para sus clústeres de Amazon ECS y Amazon EKS, incluidos ejemplos de diferentes configuraciones.
Sin servidor	Registros y métricas del sistema y de las aplicaciones para sus funciones de Lambda y consideraciones para la personalización.

Esta guía proporciona una solución de registro y monitoreo que aborda CloudWatchAWS los servicios relacionados en las siguientes áreas:

- Planificación de la CloudWatch implementación— Consideraciones para planificar la CloudWatch implementación y orientación sobre la centralización de CloudWatch la configuración.

- Configuración de CloudWatch agente para instancias EC2 y en los servidores de las instalaciones— detalles CloudWatch de configuración para el registro y las métricas a nivel de sistema y aplicación.
- Enfoques de instalación de agentes de CloudWatch para Amazon EC2 y servidores locales— Métodos para instalar el CloudWatch agente, incluida la implementación automatizada mediante Systems Manager en varias regiones y cuentas.
- Registro y supervisión en Amazon ECS — Guía CloudWatch para configurar el registro y las métricas a nivel de clúster y aplicación en Amazon ECS.
- Registro y monitoreo en Amazon EKS — Guía CloudWatch para configurar el registro y las métricas a nivel de clúster y aplicación en Amazon EKS.
- Supervisión de Prometheus en Amazon EKS— Presenta y compara Amazon Managed Service for Prometheus con la monitorización de CloudWatch Container Insights para Prometheus.
- Registro y métricas paraAWS Lambda— Guía CloudWatch para configurar las funciones de Lambda.
- Búsqueda y análisis de registros CloudWatch— Métodos para analizar sus registros mediante Amazon CloudWatch Application Insights, CloudWatch Logs Insights y ampliar el análisis de registros a Amazon OpenSearch Service.
- Opciones alarmantes con CloudWatch— Presenta la detección de CloudWatch alarmas y CloudWatch anomalías y proporciona orientación sobre la creación y configuración de alarmas.
- Supervisión de la disponibilidad de aplicaciones y servicios— Presenta y compara las comprobaciones de estado de CloudWatch Synthetics y Route 53 para la supervisión automática de la disponibilidad.
- Aplicaciones de rastreo conAWS X-Ray— Introducción y configuración del rastreo de aplicaciones mediante X-Ray para Amazon EC2, Amazon ECS, Amazon EKS y Lambda
- Paneles y visualizaciones con CloudWatch— Introducción a los CloudWatch paneles para mejorar la observabilidad en todasAWS las cargas de trabajo.
- Integración con CloudWatchAWSServicios de— Explica cómo CloudWatch se integra con variosAWS servicios.
- Amazon Managed Grafana para paneles y visualización— Presenta y compara Amazon Managed Grafana con CloudWatch para paneles y visualización.

En esta guía se utilizan ejemplos de implementación en estas áreas y también están disponibles en el GitHub repositorio deAWS muestras.

Resultados empresariales específicos

Creación de una solución de registro y monitorización diseñada para elAWSLa nube es fundamental para lograr elseis ventajas de la computación en la nube. Su solución de registro y supervisión debería ayudar a su organización de TI a lograr resultados empresariales que beneficien a sus procesos empresariales, socios comerciales, empleados y clientes. Puede esperar los cuatro resultados siguientes después de implementar una solución de registro y supervisión alineada con elAWSMarco de Well-Architected:

Acelere la preparación operativa

Habilitar una solución de registro y supervisión es un componente importante de la preparación de una carga de trabajo para el soporte y el uso de la producción. La preparación operativa puede convertirse rápidamente en un cuello de botella si depende demasiado de los procesos manuales y también puede reducir el tiempo de obtención de valor (TTV) de sus inversiones en TI. Un enfoque ineficaz también da como resultado una observabilidad limitada de las cargas de trabajo. Esto puede aumentar el riesgo de interrupciones prolongadas, insatisfacción del cliente y procesos empresariales fallidos.

Puede utilizar los enfoques de esta guía para estandarizar y automatizar el registro y la supervisión en elAWSCloud. A continuación, las nuevas cargas de trabajo requieren una preparación e intervención manuales mínimas para el registro y la supervisión de la producción. Esto también ayuda a reducir el tiempo y los pasos necesarios para crear estándares de registro y supervisión a escala para diferentes cargas de trabajo en varias cuentas y regiones.

Mejora la excelencia operativa

Esta guía proporciona múltiples prácticas recomendadas para el registro y la supervisión que ayudan a diversas cargas de trabajo a cumplir los objetivos empresariales yoperativa excelencia. Esta guía también proporcionaejemplos detallados y plantillas reutilizables de código abiertoque puede utilizar con un enfoque de infraestructura como código (iAC) para implementar una solución de registro y supervisión bien diseñada medianteAWSServicios de . Mejorar la excelencia operativa es iterativa y requiere una mejora continua. La guía proporciona sugerencias sobre cómo mejorar continuamente las prácticas de registro y supervisión.

Mejore la visibilidad operativa

Es posible que sus procesos y aplicaciones empresariales estén soportados por distintos recursos de TI y alojados en distintos tipos de cómputo, ya sea en las instalaciones o en elAWSCloud. Su visibilidad operativa puede verse limitada por implementaciones incoherentes e incompletas de su estrategia de registro y supervisión. La adopción de un enfoque integral de registro y supervisión le ayuda a identificar, diagnosticar y responder rápidamente a los problemas de las cargas de trabajo. Esta guía le ayuda a diseñar e implementar enfoques para mejorar su visibilidad operativa completa y reducir el tiempo medio de resolución de fallos (MTTR). Un enfoque integral de registro y supervisión también ayuda a su organización a mejorar la calidad del servicio, mejorar la experiencia del usuario final y cumplir los acuerdos de nivel de servicio (SLA).

Escale las operaciones y reduzca los costes generales

Puede escalar las prácticas de registro y supervisión de esta guía para admitir varias regiones y cuentas, recursos de corta duración y varios entornos. La guía proporciona enfoques y ejemplos para automatizar los pasos manuales (por ejemplo, instalar y configurar agentes, monitorear métricas y notificar o tomar medidas cuando se producen problemas). Estos enfoques son útiles cuando la adopción de la nube madura y crece y necesita escalar la capacidad operativa sin aumentar las actividades o los recursos de administración de la nube.

Planificación de la CloudWatch implementación

La complejidad y el alcance de una solución de registro y supervisión dependen de varios factores, entre ellos:

- Cuántos entornos, regiones y cuentas se utilizan y cómo podría aumentar este número.
- La variedad y los tipos de sus cargas de trabajo y arquitecturas existentes.
- Los tipos de procesamiento y los sistemas operativos que deben registrarse y supervisarse.
- Si hay ubicaciones e AWS infraestructura locales.
- Los requisitos analíticos y de agregación de varios sistemas y aplicaciones.
- Requisitos de seguridad que impiden la exposición no autorizada de registros y métricas.
- Productos y soluciones que deben integrarse con su solución de registro y monitoreo para respaldar los procesos operativos.

Debe revisar y actualizar periódicamente su solución de registro y monitoreo con implementaciones de cargas de trabajo nuevas o actualizadas. Las actualizaciones del registro, la supervisión y las alarmas deben identificarse y aplicarse cuando se detecten problemas. Estos problemas se pueden identificar y prevenir de forma proactiva en el futuro.

Debe asegurarse de instalar y configurar de forma coherente el software y los servicios para capturar e ingerir registros y métricas. Un enfoque establecido de registro y supervisión utiliza servicios y soluciones de proveedores de software (ISV) múltiples AWS o independientes para diferentes dominios (por ejemplo, seguridad, rendimiento, redes o análisis). Cada dominio tiene sus propios requisitos de implementación y configuración.

Se recomienda utilizarlo CloudWatch para capturar e ingerir registros y métricas para varios sistemas operativos y tipos de procesamiento. Muchos AWS servicios se utilizan CloudWatch para registrar, monitorear y publicar registros y métricas, sin necesidad de configuración adicional. CloudWatch proporciona un agente de software que se puede instalar y configurar para diferentes sistemas operativos y entornos. En las siguientes secciones se describe cómo implementar, instalar y configurar el CloudWatch agente para varias cuentas, regiones y configuraciones:

Temas

- Utilización CloudWatch en cuentas centralizadas o distribuidas
- Administrar los archivos CloudWatch de configuración de los agentes

Utilización CloudWatch en cuentas centralizadas o distribuidas

Aunque CloudWatch está diseñado para monitorear los AWS servicios o recursos de una cuenta y región, puede usar una cuenta central para capturar registros y métricas de varias cuentas y regiones. Si usa más de una cuenta o región, debe evaluar si desea utilizar el enfoque de cuentas centralizadas o una cuenta individual para capturar registros y métricas. Por lo general, se requiere un enfoque híbrido para las implementaciones con varias cuentas y regiones a fin de cumplir con los requisitos de los propietarios de seguridad, análisis, operaciones y cargas de trabajo.

En la siguiente tabla, se muestran las áreas que se deben tener en cuenta a la hora de elegir un enfoque centralizado, distribuido o híbrido.

Estructuras de cuentas	Su organización puede tener varias cuentas independientes (por ejemplo, cuentas para cargas de trabajo de producción y no relacionadas con la producción) o miles de cuentas para aplicacio nes individuales en entornos específicos. Le recomendamos que mantenga los registros y las métricas de las aplicaciones en la cuenta en la que se ejecuta la carga de trabajo, lo que permite a los propietarios de la carga de trabajo acceder a los registros y las métricas. Esto les permite desempeñar un papel activo en el registro y la supervisión. También le recomendamos que utilice una cuenta de registro independiente para agregar todos los registros de carga de trabajo para su análisis, agregación, tendencias y operacion es centralizadas. También se pueden usar cuentas de registro independientes para la seguridad, el archivado, la supervisión y el análisis.
Requisitos de acceso	Los miembros del equipo (por ejemplo, los propietarios de las cargas de trabajo o los desarrolladores) necesitan acceder a los registros y las métricas para solucionar problemas y realizar mejoras. Los registros deben mantenerse en la cuenta de la carga de trabajo para facilitar el acceso y la solución de problemas. Si los registros y las métricas se mantienen en una cuenta independi ente de la carga de trabajo, es posible que los usuarios tengan que alternar de una cuenta a otra con regularidad.

	El uso de una cuenta centralizada proporciona información de registro a los usuarios autorizados sin conceder acceso a la cuenta de carga de trabajo. Esto puede simplificar los requisitos de acceso para las cargas de trabajo analíticas cuando se requiere la agregación de las cargas de trabajo que se ejecutan en varias cuentas. La cuenta de registro centralizada también puede tener opciones alternativas de búsqueda y agregación, como un clúster de Amazon OpenSearch Service. Amazon OpenSearch Service proporciona un control de acceso detallado hasta el nivel de campo para tus registros. Un control de acceso detallado es important e cuando se dispone de datos sensibles o confidenciales que requieren permisos y accesos especializados.
Operaciones	Muchas organizaciones cuentan con un equipo de operaciones y seguridad centralizado o con una organización externa de apoyo operativo que requiere acceso a los registros para su supervisión. El registro y la supervisión centralizados pueden facilitar la identific ación de tendencias, la búsqueda, la agregación y la realización de análisis en todas las cuentas y cargas de trabajo. Si su organizac ión utiliza el enfoque de «usted lo crea, lo ejecuta» DevOps, los propietarios de las cargas de trabajo deberán registrar y supervisa r la información de sus cuentas. Es posible que se requiera un enfoque híbrido para satisfacer las operaciones y los análisis centrales, además de la propiedad distribuida de las cargas de trabajo.
Entorno	Puede optar por alojar los registros y las métricas en una ubicación central para las cuentas de producción y conservar los registros y las métricas de otros entornos (por ejemplo, de desarrollo o de pruebas) en la misma cuenta o en cuentas independientes, según los requisitos de seguridad y la arquitectura de la cuenta. Esto ayuda a evitar que un público más amplio acceda a los datos confidenciales creados durante la producción.

CloudWatch ofrece múltiples opciones para procesar los registros en tiempo real con filtros de CloudWatch suscripción. Puede utilizar los filtros de suscripción para transmitir los registros en tiempo real a AWS servicios para su procesamiento, análisis y carga personalizados en otros sistemas. Esto puede resultar especialmente útil si adoptas un enfoque híbrido en el que tus registros y métricas estén disponibles en cuentas y regiones individuales, además de en una cuenta y una región centralizadas. La siguiente lista proporciona ejemplos de AWS servicios que se pueden utilizar para ello:

- Amazon Data Firehose: Firehose proporciona una solución de streaming que escala y cambia el tamaño automáticamente en función del volumen de datos que se esté produciendo. No necesita gestionar el número de fragmentos de una transmisión de datos de Amazon Kinesis y puede conectarse directamente a Amazon Simple Storage Service (Amazon S3), Amazon Service o Amazon OpenSearch Redshift sin necesidad de codificación adicional. Firehose es una solución eficaz si desea centralizar sus registros en esos servicios. AWS
- Amazon Kinesis Data Streams: Kinesis Data Streams es una solución adecuada si necesita integrarse con un servicio que Firehose no admite e implementar una lógica de procesamiento adicional. Puede crear un destino de Amazon CloudWatch Logs en sus cuentas y regiones que especifique una transmisión de datos de Kinesis en una cuenta central y una función AWS Identity and Access Management (IAM) que le conceda permiso para colocar registros en la transmisión. Kinesis Data Streams proporciona una zona de aterrizaje flexible y abierta para sus datos de registro que, a su vez, puede ser consumida por diferentes opciones. Puede leer los datos de registro de Kinesis Data Streams en su cuenta, realizar el preprocesamiento y enviar los datos al destino que elija.

  Sin embargo, debe configurar las particiones de la transmisión para que tengan el tamaño adecuado para los datos de registro que se generen. Kinesis Data Streams actúa como intermediario temporal o cola para sus datos de registro y puede almacenar los datos en la transmisión de Kinesis durante un período de uno a 365 días. Kinesis Data Streams también admite la función de reproducción, lo que significa que puede reproducir los datos que no se hayan consumido.
- Amazon OpenSearch Service: CloudWatch los registros pueden transmitir los registros de un grupo de registros a un OpenSearch clúster de una cuenta individual o centralizada. Al configurar un grupo de registros para transmitir datos a un OpenSearch clúster, se crea una función Lambda en la misma cuenta y región que el grupo de registros. La función Lambda debe tener una conexión de red con el OpenSearch clúster. Puede personalizar la función Lambda para realizar un preprocesamiento adicional, además de personalizar la ingesta en Amazon Service.

OpenSearch El registro centralizado con Amazon OpenSearch Service facilita el análisis, la búsqueda y la solución de problemas en varios componentes de la arquitectura de la nube.

- Lambda: si usa Kinesis Data Streams, debe aprovisionar y administrar los recursos de cómputo que consumen datos de su transmisión. Para evitarlo, puede transmitir los datos de registro directamente a Lambda para su procesamiento y enviarlos a un destino según su lógica. Esto significa que no necesita aprovisionar ni administrar los recursos de cómputo para procesar los datos entrantes. Si decide usar Lambda, asegúrese de que la solución sea compatible con las cuotas de Lambda.

Es posible que necesite procesar o compartir los datos de registro almacenados en CloudWatch Logs en formato de archivo. Puede crear una tarea de exportación para exportar un grupo de registros a Amazon S3 para un intervalo de fechas o horas específico. Por ejemplo, puede optar por exportar los registros a diario a Amazon S3 para realizar análisis y auditorías. Lambda se puede utilizar para automatizar esta solución. También puede combinar esta solución con la replicación de Amazon S3 para enviar y centralizar los registros de varias cuentas y regiones a una sola cuenta y región centralizadas.

La configuración del CloudWatch agente también puede especificar un `credentials` campo en la `agent`sección. Esto especifica una función de IAM que se utilizará al enviar métricas y registros a una cuenta diferente. Si se especifica, este campo contiene el `role_arn` parámetro. Este campo se puede usar cuando solo necesita el registro y la supervisión centralizados en una cuenta y región centralizadas específicas.

También puede usar el SDK de AWS para escribir su propia aplicación de procesamiento personalizada en el idioma que prefiera, leer los registros y las métricas de sus cuentas y enviar datos a una cuenta centralizada u otro destino para su posterior procesamiento y supervisión.

Administrar los archivos CloudWatch de configuración de los agentes

Le recomendamos que cree una configuración de CloudWatch agente de Amazon estándar que incluya los registros y las métricas del sistema que desee capturar en todas sus instancias de Amazon Elastic Compute Cloud (Amazon EC2) y servidores locales. Puede utilizar el asistente para archivos de configuración del CloudWatch agente como ayuda para crear el archivo de configuración. Puede ejecutar el asistente de configuración varias veces para generar configuraciones únicas para diferentes sistemas y entornos. También puede modificar el archivo

de configuración o crear variantes mediante el esquema del archivo de configuración. El archivo de configuración del CloudWatch agente se puede almacenar en los parámetros del AWS Systems Manager Parameter Store. Puede crear parámetros de almacén de parámetros independientes si tiene varios archivos de configuración de CloudWatch agentes. Si utiliza varias cuentas de AWS o regiones de AWS, debe gestionar y actualizar los parámetros del almacén de parámetros en cada cuenta y región. Como alternativa, puede gestionar sus CloudWatch configuraciones de forma centralizada como archivos en Amazon S3 o en la herramienta de control de versiones que prefiera.

El `amazon-cloudwatch-agent-ctl` script incluido con el CloudWatch agente le permite especificar un archivo de configuración, un parámetro del almacén de parámetros o la configuración predeterminada del agente. La configuración predeterminada se ajusta al conjunto de métricas básico predefinido y configura el agente para que informe las métricas de memoria y espacio en disco. CloudWatch Sin embargo, no incluye ninguna configuración de archivos de registro. La configuración predeterminada también se aplica si utiliza la configuración rápida de Systems Manager para el CloudWatch agente.

Como la configuración predeterminada no incluye el registro y no está personalizada según sus requisitos, le recomendamos que cree y aplique sus propias CloudWatch configuraciones, personalizadas según sus requisitos.

Administrar CloudWatch las configuraciones

De forma predeterminada, CloudWatch las configuraciones se pueden almacenar y aplicar como parámetros del almacén de parámetros o como archivos CloudWatch de configuración. La mejor opción dependerá de sus requisitos. En esta sección, analizamos los pros y los contras de estas dos opciones. También se detalla una solución representativa para administrar los archivos de CloudWatch configuración de varias cuentas y regiones de AWS.

Parámetros del almacén de parámetros de Systems Manager

El uso de los parámetros del almacén de parámetros para administrar CloudWatch las configuraciones funciona bien si tiene un único archivo de configuración de CloudWatch agente estándar que desea aplicar y administrar en un conjunto reducido de cuentas y regiones de AWS. Al almacenar CloudWatch las configuraciones como parámetros del almacén de parámetros, puede utilizar la herramienta de configuración del CloudWatch agente (`amazon-cloudwatch-agent-ctl`en Linux) para leer y aplicar la configuración desde el almacén de parámetros sin necesidad de copiar el archivo de configuración en la instancia. Puede utilizar el AmazonCloudWatch documento ManageAgent Systems Manager Command para actualizar la CloudWatch configuración en varias

instancias de EC2 en una sola ejecución. Como los parámetros del almacén de parámetros son regionales, debe actualizar y mantener los CloudWatch parámetros del almacén de parámetros en cada región de AWS y cuenta de AWS. Si tiene varias CloudWatch configuraciones que desea aplicar a cada instancia, debe personalizar el documento AmazonCloudWatch- ManageAgent Command para incluir estos parámetros.

CloudWatch archivos de configuración

Administrar CloudWatch las configuraciones como archivos puede funcionar bien si tiene muchas cuentas y regiones de AWS y administra varios archivos CloudWatch de configuración. Con este enfoque, puede buscarlos, organizarlos y administrarlos en una estructura de carpetas. Puede aplicar reglas de seguridad a carpetas o archivos individuales para limitar y conceder el acceso, como permisos de actualización y lectura. Puede compartirlos y transferirlos fuera de AWS para colaborar. Puede controlar las versiones de los archivos para realizar un seguimiento de los cambios y gestionarlos. Puede aplicar CloudWatch las configuraciones de forma colectiva copiando los archivos de configuración en el directorio de configuración del CloudWatch agente sin aplicar cada archivo de configuración de forma individual. Para Linux, el directorio CloudWatch de configuración se encuentra en`/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d`. Para Windows, el directorio de configuración se encuentra en`C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs`.

Al iniciar el CloudWatch agente, el agente agrega automáticamente cada archivo que se encuentra en estos directorios para crear un archivo de configuración CloudWatch compuesto. Los archivos de configuración deben almacenarse en una ubicación central (por ejemplo, un bucket de S3) a la que puedan acceder las cuentas y regiones necesarias. Se proporciona un ejemplo de solución que utiliza este enfoque.

Organizar CloudWatch las configuraciones

Independientemente del enfoque utilizado para gestionar CloudWatch las configuraciones, organícelas CloudWatch . Puede organizar las configuraciones en rutas de archivos o almacenes de parámetros mediante un enfoque como el siguiente.

/config/standard/windows/ec2	Almacene los archivos de CloudWatch configuración estándar específicos de Windows para Amazon EC2. En esta carpeta, puede clasificar con más detalle las configuraciones de su sistema operativo (SO) estándar para

	diferentes versiones de Windows, tipos de instancias de EC2 y entornos.
/config/standard/windows/onpremises	Almacene los archivos de configuración estándar específicos de Windows para los servidores locales. CloudWatch También puede clasificar con más detalle las configuraciones de sistema operativo estándar para las diferentes versiones, tipos de servidores y entornos de Windows en esta carpeta.
/config/standard/linux/ec2	Guarde sus archivos de CloudWatch configuración estándar específicos de Linux para Amazon EC2. En esta carpeta, puede clasificar con más detalle la configuración estándar del sistema operativo para diferentes distribuciones de Linux, tipos de instancias EC2 y entornos.
/config/standard/linux/onpremises	Guarde los archivos de configuración estándar específicos de Linux para los servidores locales. CloudWatch En esta carpeta, puede clasificar con más detalle la configuración estándar del sistema operativo para diferentes distribuciones, tipos de servidores y entornos de Linux.
/config/ecs	CloudWatch Guarde los archivos de configuración específicos de Amazon Elastic Container Service (Amazon ECS) si utiliza instancias de contenedor de Amazon ECS. Estas configuraciones se pueden añadir a las configuraciones estándar de Amazon EC2 para el registro y la supervisión a nivel de sistemas específicos de Amazon ECS.

/config/ <application_name>	Guarde los archivos de configuración específicos de la aplicación CloudWatch . Puede clasificar aún más sus aplicaciones con carpetas y prefijos adicionales para los entornos y las versiones.

Ejemplo: almacenar los archivos CloudWatch de configuración en un bucket de S3

En esta sección se proporciona un ejemplo del uso de Amazon S3 para almacenar los archivos de CloudWatch configuración y un manual personalizado de Systems Manager para recuperar y aplicar los archivos de CloudWatch configuración. Este enfoque puede abordar algunos de los desafíos que implica el uso de los parámetros del almacén de parámetros de Systems Manager para CloudWatch la configuración a escala:

- Si utiliza varias regiones, debe sincronizar las actualizaciones de CloudWatch configuración en el almacén de parámetros de cada región. El almacén de parámetros es un servicio regional y se debe actualizar el mismo parámetro en cada región que utilice el CloudWatch agente.
- Si tiene varias CloudWatch configuraciones, debe iniciar la recuperación y la aplicación de cada configuración del almacén de parámetros. Debe recuperar individualmente cada CloudWatch configuración del almacén de parámetros y también actualizar el método de recuperación cada vez que añada una nueva configuración. Por el contrario, CloudWatch proporciona un directorio de configuración para almacenar los archivos de configuración y aplica cada configuración del directorio, sin necesidad de especificarlas individualmente.
- Si utiliza varias cuentas, debe asegurarse de que cada cuenta nueva tenga las CloudWatch configuraciones necesarias en su almacén de parámetros. También debe asegurarse de que cualquier cambio de configuración se aplique a estas cuentas y sus regiones en el futuro.

Puede almacenar CloudWatch las configuraciones en un depósito de S3 al que pueda acceder desde todas sus cuentas y regiones. A continuación, puede copiar estas configuraciones del bucket de S3 al directorio de CloudWatch configuración mediante los manuales de automatización de Systems Manager y el administrador de estado de Systems Manager. Puede usar la plantilla de CloudFormation AWS de cloudwatch-config-s3 compartimentos .yaml para crear un depósito de S3 al que se pueda acceder desde varias cuentas de una organización en AWS Organizations. La plantilla

incluye un `OrganizationID` parámetro que otorga acceso de lectura a todas las cuentas de su organización.

El manual de ejemplo ampliado de Systems Manager, que se incluye en la sección Configurar State Manager and Distributor para el despliegue y la configuración de los CloudWatch agentes de esta guía, está configurado para recuperar archivos mediante el depósito de S3 creado por la plantilla AWS cloudwatch-config-s3-bucket.yaml. CloudFormation

Como alternativa, puede utilizar un sistema de control de versiones (por ejemplo, GitHub o AWS CodeCommit) para almacenar los archivos de configuración. Si desea recuperar automáticamente los archivos de configuración almacenados en un sistema de control de versiones, debe administrar o centralizar el almacenamiento de credenciales y actualizar el manual de automatización de Systems Manager que se utiliza para recuperar las credenciales en sus cuentas y regiones.

Configuración de CloudWatch agente para instancias EC2 y en los servidores de las instalaciones

Muchas organizaciones ejecutan cargas de trabajo en servidores físicos y máquinas virtuales (VM). Estas cargas de trabajo suelen ejecutarse en diferentes sistemas operativos que tienen requisitos de instalación y configuración únicos para capturar e ingerir métricas.

Si elige utilizar instancias EC2, puede tener un alto nivel de control sobre la configuración de la instancia y del sistema operativo. Sin embargo, este mayor nivel de control y responsabilidad requiere que supervise y ajuste las configuraciones para lograr un uso más eficiente. Puede mejorar su eficacia operativa estableciendo estándares de registro y supervisión y aplicando un enfoque estándar de instalación y configuración para capturar e ingerir registros y métricas.

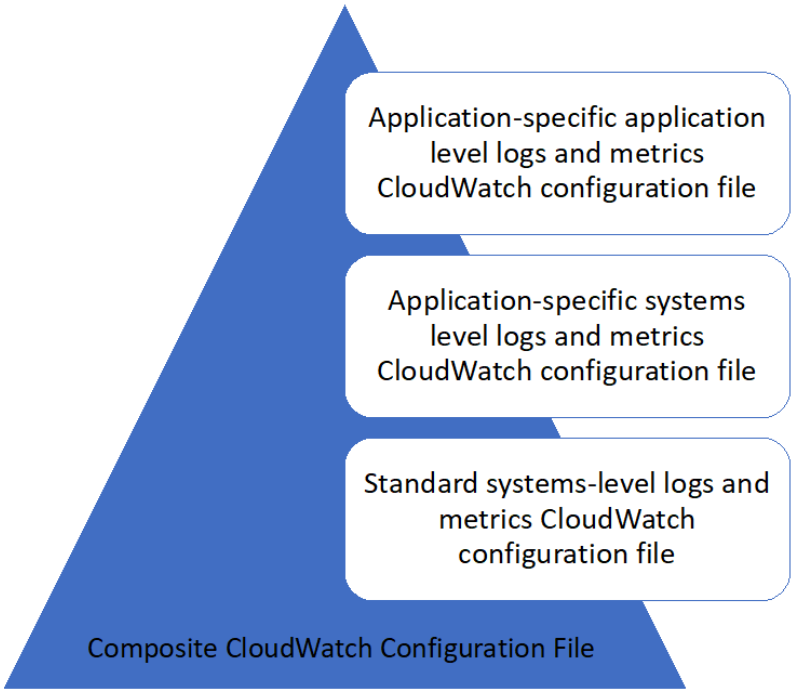
Organizations que migran o amplían sus inversiones en TI alAWSLa nube puede aprovechar CloudWatch para lograr una solución unificada de registro y monitoreo. CloudWatch precio significa que pagas de forma incremental las métricas y los registros que quieres capturar. También puede capturar registros y métricas para servidores locales mediante un método similar. CloudWatch proceso de instalación del agente como el de Amazon EC2.

Antes de comenzar a instalar e implementar CloudWatch, asegúrese de evaluar las configuraciones de registro y métricas de sus sistemas y aplicaciones. Asegúrese de definir los registros y las métricas estándar que necesita capturar para los sistemas operativos que desea utilizar. Los registros y las métricas del sistema son la base y el estándar de una solución de registro y supervisión porque son generados por el sistema operativo y son diferentes para Linux y Windows. Hay métricas y archivos de registro importantes disponibles en todas las distribuciones de Linux, además de aquellos que son específicos de una versión o distribución de Linux. Esta variación también se produce entre las distintas versiones de Windows.

Configuración de CloudWatch agente

CloudWatch captura métricas y registros de Amazon EC2 y en los servidores de las instalaciones mediante Agentes de CloudWatch y archivos de configuración del agente que son específicos de cada sistema operativo. Le recomendamos que defina la configuración estándar de captura de registros y métricas de su organización antes de comenzar a instalar el CloudWatch agente a escala en sus cuentas.

Puede combinar varios CloudWatch configuraciones de agente para formar un compuesto CloudWatch configuración del agente de. Un enfoque recomendado es definir y dividir las configuraciones de sus registros y métricas a nivel de sistema y aplicación. El siguiente diagrama ilustra cómo se pueden combinar varios tipos de archivos de configuración de CloudWatch para diferentes requisitos para formar una configuración compuesta de CloudWatch:



Estos registros y métricas también se pueden clasificar y configurar más para entornos o requisitos específicos. Por ejemplo, podría definir un subconjunto más pequeño de registros y métricas con menor precisión para entornos de desarrollo no regulados y un conjunto más grande y completo con mayor precisión para entornos de producción regulados.

Configuración de la captura de registros para instancias EC2

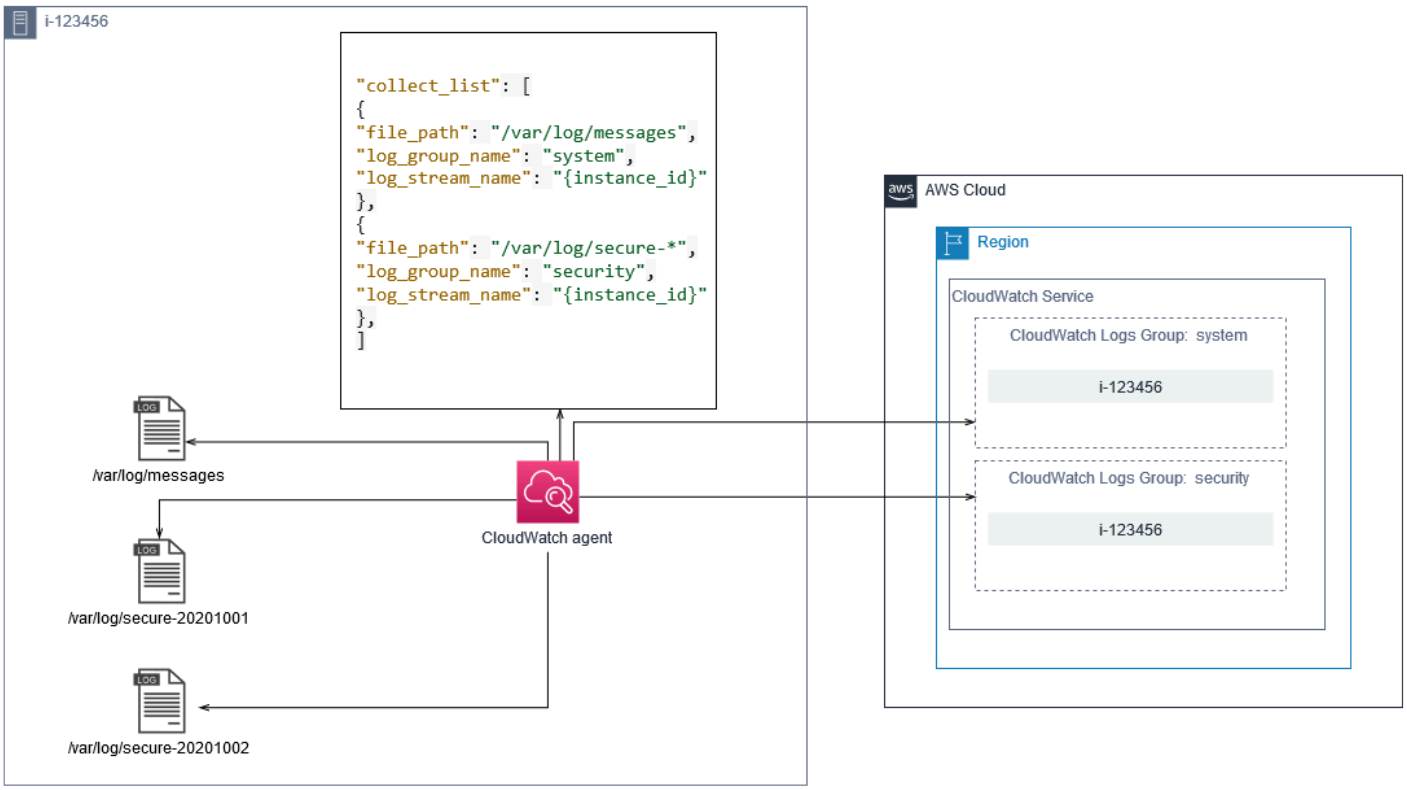
De forma predeterminada, Amazon EC2 no supervisa ni captura archivos de registro. En su lugar, los archivos de registro se capturan e ingieren en CloudWatch Registros de la CloudWatch software del agente instalado en la instancia EC2,AWSAPI, oAWS Command Line Interface(AWS CLI). Recomendamos utilizar el CloudWatch agente para ingerir archivos de registro en CloudWatch Registros de Amazon EC2 y en los servidores de las instalaciones.

Puede buscar y filtrar registros, así como extraer métricas y ejecutar la automatización basada en el parche de patrones de los archivos de registro de CloudWatch. CloudWatch admite opciones de sintaxis de patrones y filtros de texto sin formato, delimitados por espacios y con formato JSON, y los registros con formato JSON proporcionan la mayor flexibilidad. Para aumentar las opciones de filtrado y análisis, debe utilizar una salida de registro con formato en lugar de texto sin formato.

La CloudWatch agente utiliza un archivo de configuración que define los registros y las métricas que se van a enviar a CloudWatch. CloudWatch luego captura cada archivo de registro comoflujo de registroy agrupa estos flujos de registro en ungrupo de registros. Esto le ayuda a realizar operaciones en los registros de las instancias EC2, como buscar una cadena coincidente.

El nombre del flujo de registro predeterminado es el mismo que el ID de instancia de EC2 y el nombre del grupo de registros predeterminado es el mismo que la ruta del archivo de registro. El nombre del flujo de registro debe ser único dentro del CloudWatch grupo de registros. Puede usar`instance_id`,`hostname`,`local_hostname`, o bien`ip_address`para sustitución dinámica en el flujo de registros y nombres de grupos de registros, lo que significa que puede utilizar el mismo CloudWatch archivo de configuración del agente en varias instancias EC2.

En el siguiente diagrama se muestra un CloudWatch configuración de agente para capturar registros. El grupo de registros se define mediante los archivos de registro capturados y contiene flujos de registro independientes para cada instancia de EC2 debido a que`{instance_id}`se utiliza para el nombre del flujo de registro y los ID de instancia de EC2 son únicos.



Los grupos de registros definen la retención, las etiquetas, la seguridad, los filtros de métricas y el ámbito de búsqueda de los flujos de registro que contienen. El comportamiento de agrupación predeterminado basado en el nombre del archivo de registro le ayuda a buscar, crear métricas y alarmas de datos específicos de un archivo de registro en las instancias EC2 de una cuenta y una región. Debe evaluar si se requiere un mayor refinamiento de grupos de registros. Por ejemplo, es posible que varias unidades de negocio compartan tu cuenta y tengan distintos propietarios técnicos o de operaciones. Esto significa que debe refinar aún más el nombre del grupo de registros para reflejar la separación y la propiedad. Este enfoque le permite concentrar el análisis y la solución de problemas en la instancia EC2 correspondiente.

Si varios entornos utilizan una cuenta, puede separar el registro de las cargas de trabajo que se ejecutan en cada entorno. En la tabla siguiente se muestra una convención de nomenclatura de grupos de registros que incluye la unidad de negocio, el proyecto o la aplicación y el entorno.

Nombre de grupo de registro	`/<Business unit>/<Project or application name>/<Environment>/<Log file name>`

Nombre del flujo de registros	`<EC2 instance ID>`

También puede agrupar todos los archivos de registro de una instancia EC2 en el mismo grupo de registros. Esto facilita la búsqueda y el análisis en un conjunto de archivos de registro de una única instancia EC2. Esto resulta útil si la mayoría de las instancias EC2 atienden una aplicación o carga de trabajo y cada instancia EC2 cumple un propósito específico. En la tabla siguiente se muestra cómo se puede dar formato a su grupo de registros y nombres de flujos de registros para admitir este enfoque.

Nombre de grupo de registro	`/<Business unit>/<Project or application name>/<Environment>/<EC2 instance ID>`
Nombre del flujo de registros	`<Log file name>`

Configuración de la captura de métricas para instancias EC2

De forma predeterminada, las instancias EC2 están habilitadas para la monitorización básica yconjunto estándar de métricas(por ejemplo, métricas relacionadas con CPU, red o almacenamiento de información) se envía automáticamente a CloudWatch cada cinco minutos. CloudWatch Las métricas pueden variar en función de la familia de instancias, por ejemplo,instancias de rendimiento ampliabletienen métricas para créditos de CPU. Las métricas estándar de Amazon EC2 se incluyen en el precio de la instancia. Si habilitamonitorización detalladaEn las instancias EC2, puede recibir datos en periodos de un minuto. La frecuencia del período afecta a los costes de CloudWatch, así que asegúrese de evaluar si se requiere una supervisión detallada para todas o solo algunas de sus instancias EC2. Por ejemplo, podría habilitar la supervisión detallada de las cargas de trabajo de producción pero utilizar la supervisión básica para cargas de trabajo que no son de producción.

Los servidores locales no incluyen métricas predeterminadas para CloudWatch y debe utilizar el CloudWatch agente,AWS CLI, o bienAWSSDK para capturar métricas. Esto significa que debe definir las métricas que desea capturar (por ejemplo, utilización de la CPU) en el CloudWatch archivo de configuración. Puede crear un único CloudWatch archivo de configuración que incluye las

métricas de instancias EC2 estándar para los servidores locales y lo aplica además de su estándar CloudWatch Configuración de .

Métricasen CloudWatch se definen de forma exclusiva mediante el nombre de la métrica y cero o varias dimensiones y se agrupan de forma exclusiva en un espacio de nombres de métricas. Métricas proporcionadas por unAWSservice tiene un espacio de nombres que comienza con`AWS`(por ejemplo,`AWS/EC2`), y noAWSLas métricas se consideran métricas de personalizadas. Métricas que configura y captura con el CloudWatch agente se consideran métricas personalizadas. Porque el número de métricas creadas afecta a su CloudWatch costes, debe evaluar si cada métrica es necesaria para todas o solo algunas de sus instancias EC2. Por ejemplo, podría definir un conjunto completo de métricas para cargas de trabajo de producción pero utilizar un subconjunto más pequeño de estas métricas para cargas de trabajo que no son de producción.

`CWAgente`s el espacio de nombres predeterminado para las métricas publicadas por el CloudWatch agente. De forma similar a los grupos de registros, el espacio de nombres de métricas organiza un conjunto de métricas para que se puedan encontrar juntas en un solo lugar. Debe modificar el espacio de nombres para reflejar una unidad de negocio, proyecto o aplicación y entorno (por ejemplo,`/<Business unit>/<Project or application name>/<Environment>`). Este enfoque resulta útil si varias cargas de trabajo no relacionadas utilizan la misma cuenta. También puede correlacionar la convención de nomenclatura del espacio de nombres con su CloudWatch convención de nombres de grupos de registros.

Las métricas también se identifican por sus dimensiones, que ayudan a analizarlas en función de un conjunto de condiciones y son las propiedades en las que se registran las observaciones. Amazon EC2 incluyemétricas separadaspara instancias EC2 con`InstanceId`y`AutoScalingGroupName`Dimensiones. También recibes métricas con el`ImageId`y`InstanceType`dimensiones si habilita la monitorización detallada. Por ejemplo, Amazon EC2 proporciona una métrica de instancia EC2 independiente para la utilización de la CPU con el`InstanceId`dimensiones, además de una métrica de utilización de CPU separada para el`InstanceType`Dimensión. Esto le ayuda a analizar la utilización de la CPU para cada instancia EC2 única, además de todas las instancias EC2 de un determinadotipo de instancia.

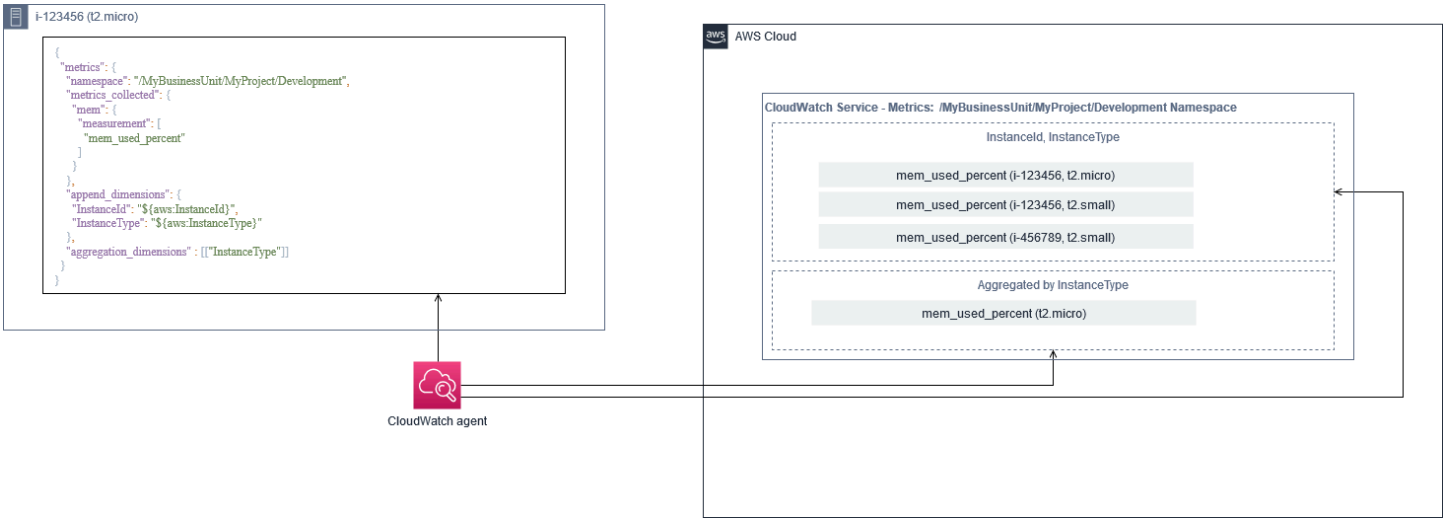
La adición de más dimensiones aumenta la capacidad de análisis pero también aumenta los costes generales, porque cada combinación de métrica y valor de dimensión única da como resultado una nueva métrica. Por ejemplo, si crea una métrica para el porcentaje de utilización de memoria frente al`InstanceId`, esta es una nueva métrica para cada instancia de EC2. Si su organización ejecuta miles de instancias EC2, esto provoca miles de métricas y se traduce en costos más elevados. Para controlar y predecir los costes, asegúrese de determinar la cardinalidad de la métrica y qué

dimensiones añaden más valor. Por ejemplo, podría definir un conjunto completo de dimensiones para las métricas de carga de trabajo de producción, pero un subconjunto más pequeño de estas dimensiones para cargas de trabajo que no son de producción.

Puede utilizar el`append_dimensions`para añadir dimensiones a una o todas las métricas definidas en su CloudWatch Configuración de . También puede añadir dinámicamente el`ImageId`,`InstanceId`,`InstanceType`, y`AutoScalingGroupName`a todas las métricas de tu CloudWatch Configuración de . Alternativamente, puede agregar un nombre y un valor de dimensión arbitrarios para métricas específicas mediante el`append_dimensions`propiedad de esa métrica. CloudWatch también puede agregar estadísticas sobre las dimensiones métricas definidas con el`aggregation_dimensions`propiedad.

Por ejemplo, podría agregar la memoria utilizada en la`InstanceType`para ver la memoria media utilizada por todas las instancias EC2 para cada tipo de instancia. Si utiliza`t2.micro`instancias que se ejecutan en una región, puede determinar si las cargas de trabajo utilizando el`t2.micro`están sobreutilizando o infrautilizando la memoria proporcionada. La infrautilización podría ser un signo de cargas de trabajo que utilizan clases EC2 con capacidad de memoria no necesaria. En cambio, la sobreutilización podría ser un signo de cargas de trabajo que utilizan clases de Amazon EC2 con memoria insuficiente.

En el siguiente diagrama se muestra un ejemplo CloudWatch configuración de métricas que utiliza un espacio de nombres personalizado, dimensiones añadidas y agregación mediante`InstanceType`.



Nivel de sistema CloudWatch configuración

Las métricas y los registros a nivel de sistemas son un componente central de una solución de monitoreo y registro, y el CloudWatch agent tiene opciones de configuración específicas para Windows y Linux.

Le recomendamos que utilice elAsistente de archivos de configuración de Cloudo esquema de archivo de configuración para definir el CloudWatch archivo de configuración de agente para cada SO que planea admitir. Los registros y métricas de nivel del SO específicos de la carga de trabajo adicionales se pueden definir por separado CloudWatch archivos de configuración y anexados a la configuración estándar. Estos archivos de configuración exclusivos deben almacenarse por separado en un bucket de S3, donde las instancias EC2 pueden recuperarlos. Un ejemplo de configuración de bucket de S3 para este fin se describe en elAdministrar CloudWatch las configuracionessección de esta guía. Puede recuperar y aplicar automáticamente estas configuraciones mediante State Manager y Distributor.

Configuración de registros de nivel de sistema

Los registros a nivel de sistema son esenciales para diagnosticar y solucionar problemas en las instalaciones o en elAWSCloud. El enfoque de captura de registros debe incluir cualquier registro de sistema y seguridad generados por el sistema operativo. Los archivos de registro generados por el sistema operativo pueden variar en función de la versión del sistema operativo.

La CloudWatch el agente admite la supervisión de los registros de eventos de Windows proporcionando el nombre del registro de eventos. Puede elegir qué registros de eventos de Windows desea supervisar (por ejemplo,`System`,`Application`, o bien`Security`).

Los registros del sistema, las aplicaciones y la seguridad de los sistemas Linux se almacenan normalmente en el`/var/log`directorio. En la siguiente tabla se definen los archivos de registro predeterminados comunes que debe supervisar, pero debe comprobar la`/etc/rsyslog.conf`o`/etc/syslog.conf`para determinar la configuración específica de los archivos de registro de su sistema.

Distribución Fedora (Amazon Linux, CentOS, Red Hat Enterprise Linux)	`/var/log/boot.log*` — Registro de arranque
	`/var/log/dmesg` — Registro del kernel

	`/var/log/secure` — Registro de seguridad y autenticación
	`/var/log/messages` — Registro general del sistema
	`/var/log/cron*` — Registros Cron
	`/var/log/cloud-init-output.log` — Salida de`Userdata`scripts de inicio
Debian (Ubuntu)	`/var/log/syslog` — Registro de arranque
	`/var/log/cloud-init-output.log` — Salida de`Userdata`scripts de inicio
	`/var/log/auth.log` — Registro de seguridad y autenticación
	`/var/log/kern.log` — Registro del kernel

Es posible que su organización también tenga otros agentes o componentes del sistema que generan registros que desea supervisar. Debe evaluar y decidir qué archivos de registro generan estos agentes o aplicaciones, e incluirlos en la configuración identificando la ubicación de sus archivos. Por ejemplo, debe incluir Systems Manager y CloudWatch registros de agente en la configuración. En la tabla siguiente se proporciona la ubicación de estos registros de agentes para Windows y Linux.

Windows	Agente de CloudWatch	`$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log`
	Agente de Systems Manager	`%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log`

		%PROGRAMDATA%\Amazon\SSM\Logs\errors.log %PROGRAMDATA%\Amazon\SSM\Logs\audits\amazon-ssm-agent-audit-YYYY-MM-DD
Linux	Agente de CloudWatch	/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
	Agente de Systems Manager	/var/log/amazon/ssm/amazon-ssm-agent.log /var/log/amazon/ssm/errors.log /var/log/amazon/ssm/audits/amazon-ssm-agent-audit-YYYY-MM-DD

CloudWatch ignora un archivo de registro si el archivo de registro se define en el CloudWatch configuración del agente pero no se encuentra. Esto resulta útil cuando desea mantener una configuración de registro única para Linux, en lugar de configuraciones independientes para cada distribución. También resulta útil cuando no existe un archivo de registro hasta que el agente o la aplicación de software comience a ejecutarse.

Configuración de métricas de nivel de sistema

La utilización de memoria y espacio en disco no se incluye en las métricas estándar proporcionadas por Amazon EC2. Para incluir estas métricas, debe instalar y configurar la CloudWatch agente en sus instancias EC2. La CloudWatch El asistente de configuración del agente crea un CloudWatch configuración conmétricas predefinidasy puede añadir o eliminar métricas según sea necesario.

Asegúrese de revisar los conjuntos de métricas predefinidos para determinar el nivel adecuado que necesita.

Los usuarios finales y los propietarios de cargas de trabajo deben publicar métricas del sistema adicionales en función de los requisitos específicos de un servidor o instancia EC2. Estas definiciones de métricas deben almacenarse, versionarse y mantenerse de forma independiente CloudWatch archivo de configuración de agente y compartido en una ubicación central (por ejemplo, Amazon S3) para su reutilización y automatización.

Las métricas estándar de Amazon EC2 no se capturan automáticamente en los servidores locales. Estas métricas deben definirse en un CloudWatch archivo de configuración de agente utilizado por las instancias locales. Puede crear un archivo de configuración de métricas independiente para instancias locales con métricas como la utilización de la CPU, y añadir estas métricas al archivo de configuración de métricas estándar.

Nivel de aplicación CloudWatch configuración

Los registros y las métricas de las aplicaciones se generan mediante aplicaciones en ejecución y son específicos de la aplicación. Asegúrese de definir los registros y las métricas necesarios para supervisar adecuadamente las aplicaciones que utiliza regularmente su organización. Por ejemplo, es posible que su organización se haya estandarizado en Microsoft Internet Information Server (IIS) para aplicaciones basadas en web. Puede crear un registro y una métrica estándar CloudWatch configuración para IIS que también se puede utilizar en toda la organización. Los archivos de configuración específicos de la aplicación se pueden almacenar en una ubicación centralizada (por ejemplo, un bucket de S3) y los propietarios de la carga de trabajo o mediante recuperación automática acceden a ellos, y se copian en el CloudWatch directorio de configuración. La CloudWatch agente combina automáticamente los archivos de configuración de CloudWatch que se encuentran en el directorio de archivos de configuración de cada instancia o servidor de EC2 en un compuesto CloudWatch Configuración de . El resultado final es un CloudWatch configuración que incluye la configuración estándar a nivel de sistema de su organización, así como toda la aplicación pertinente CloudWatch configuraciones.

Los propietarios de cargas de trabajo deben identificar y configurar los archivos de registro y las métricas para todas las aplicaciones y componentes críticos.

Configuración de registros a nivel de aplicación

El registro a nivel de aplicación varía según si la aplicación es comercial off-the-shelf (COTS) o aplicación desarrollada a medida. Las aplicaciones COTS y sus componentes pueden proporcionar varias opciones de configuración y salida de registros, como nivel de detalle de registro, formato de archivo de registro y ubicación de archivos de registro. Sin embargo, la mayoría de las aplicaciones COTS o de terceros no le permiten cambiar fundamentalmente el registro (por ejemplo, actualizar el código de la aplicación para incluir sentencias de registro o formatos adicionales que no se pueden configurar). Como mínimo, debe configurar las opciones de registro para COTS o aplicaciones de terceros para registrar información de advertencia e información de nivel de error, preferiblemente en formato JSON.

Puede integrar aplicaciones desarrolladas a medida con CloudWatch Registros mediante la inclusión de los archivos de registro de la aplicación en su CloudWatch Configuración de . Las aplicaciones personalizadas proporcionan una mejor calidad y control del registro porque puede personalizar el formato de salida del registro, clasificar y separar la salida de componentes en archivos de registro independientes, además de incluir los detalles necesarios adicionales. Asegúrese de revisar y estandarizar las bibliotecas de registro y los datos y el formato necesarios para su organización para que el análisis y el procesamiento sean más fáciles.

También puede escribir a un CloudWatch Flujo de registro con el CloudWatch Registros`PutLogEvents`Llamada a la API o mediante elAWSSDK. Puede utilizar la API o el SDK para requisitos de registro personalizados, como coordinar el registro en un único flujo de registros en un conjunto distribuido de componentes y servidores. Sin embargo, la solución más fácil de mantener y más aplicable es configurar las aplicaciones para que escriban en archivos de registro y, a continuación, utilizar el CloudWatch agente para leer y transmitir los archivos de registro a CloudWatch.

También debe tener en cuenta el tipo de métricas que desea medir a partir de los archivos de registro de aplicaciones. Puede utilizar filtros métricos para medir, graficar y alarmar estos datos en un CloudWatch grupo de registros. Por ejemplo, puede utilizar un filtro de métricas para contar los intentos de inicio de sesión fallidos identificándolos en los registros.

También puede crear métricas personalizadas para sus aplicaciones desarrolladas a medida mediante elMétricas integradas de CloudWatchformatoen los archivos de registro de aplicaciones.

Configuración de métricas de nivel de aplicación

Las métricas personalizadas son métricas que no proporcionan directamenteAWSservicios para CloudWatch y se publican en un espacio de nombres personalizado en CloudWatch Métricas de . Todas las métricas de la aplicación se consideran personalizadas CloudWatch Métricas de . Las métricas de la aplicación pueden alinearse con una instancia de EC2, un componente de aplicación, una llamada a la API o incluso una función empresarial. También debes tener en cuenta la importancia y la cardinalidad de las dimensiones que eliges para tus métricas. Las dimensiones con alta cardinalidad generan un gran número de métricas personalizadas y podrían aumentar su CloudWatch .

CloudWatch le ayuda a capturar métricas a nivel de aplicación de varias formas, incluidas las siguientes:

- Capture métricas a nivel de proceso definiendo los procesos individuales que desea capturar desde elel complemento procstat.
- Una aplicación publica una métrica en Windows Performance Monitor y esta métrica se define en el CloudWatch Configuración de .
- Los filtros y patrones de métricas se aplican a los registros de una aplicación en CloudWatch.
- Una aplicación escribe en un CloudWatch Log con la CloudWatch formato métrico integradas.
- Una aplicación envía una métrica a CloudWatch a través de la API oAWSSDK.
- Una aplicación envía una métrica a unrecolectadooStatsDdaemon con una configuración CloudWatch agente.

Puede utilizar procstat para supervisar y medir los procesos de aplicación críticos con el agente de CloudWatch. Esto le ayuda a activar una alarma y tomar medidas (por ejemplo, un proceso de notificación o reinicio) si un proceso crítico ya no se está ejecutando para la aplicación. También puede medir las características de rendimiento de los procesos de aplicación y emitir una alarma si un proceso en particular actúa de forma anormal.

La supervisión de Procstat también es útil si no puedes actualizar tus aplicaciones COTS con métricas personalizadas adicionales. Por ejemplo, puede crear un`my_process`métrica que mide el`cpu_time`e incluye un personalizado`application_version`Dimensión. También puede utilizar varios CloudWatch archivos de configuración de agente de una aplicación si tiene dimensiones diferentes para métricas diferentes.

Si la aplicación se ejecuta en Windows, debe evaluar si ya publica métricas en Windows Performance Monitor. Muchas aplicaciones COTS se integran con Windows Performance Monitor, lo que le ayuda a supervisar fácilmente las métricas de las aplicaciones. CloudWatch también se integra con Windows Performance Monitor y puede capturar cualquier métrica que ya esté disponible en él.

Asegúrese de revisar el formato de registro y la información de registro proporcionada por las aplicaciones para determinar qué métricas se pueden extraer con filtros de métricas. Puede revisar los registros históricos de la aplicación para determinar cómo se representan los mensajes de error y los apagados anormales. También debe revisar los problemas notificados anteriormente para determinar si se puede capturar una métrica para evitar que el problema se repita. También debe revisar la documentación de la aplicación y pedir a los desarrolladores de aplicaciones que confirmen cómo se pueden identificar los mensajes de error.

Para las aplicaciones desarrolladas a medida, trabaje con los desarrolladores de la aplicación para definir métricas importantes que se pueden implementar mediante el CloudWatch formato métrico integradas,AWSSDK, oAWSAPI. El enfoque recomendado consiste en utilizar el formato de métricas integradas. Puede utilizar elAWSproporcionó bibliotecas de formato métrico incrustadas de código abierto para ayudarle a escribir sus declaraciones en el formato requerido. También necesitaría actualizar suespecífica de la aplicación CloudWatch configuraciónpara incluir el agente de formato de métricas integradas. Esto hace que el agente que se ejecuta en la instancia EC2 actúe como un extremo de formato de métrica incrustado local que envía métricas de formato métrico incrustado a CloudWatch.

Si sus aplicaciones ya admiten métricas de publicación para recopilarlas o en estado, puede aprovecharlas para incorporar métricas en CloudWatch.

Enfoques de instalación de agentes de CloudWatch para Amazon EC2 y servidores locales

Automatizar el CloudWatch el proceso de instalación del agente le ayuda a implementarlo de forma rápida y coherente y a capturar los registros y métricas necesarios. Existen varios enfoques para automatizar la instalación del agente de CloudWatch, incluida la compatibilidad con varias cuentas y varias regiones. Se analizan los siguientes enfoques de instalación automatizada:

- Instalación de CloudWatch agente mediante Distribuidor de Systems Manager y Systems Manager State Manager: recomendamos que utilice este enfoque si las instancias EC2 y servidores en las instalaciones están ejecutando el agente de Systems Manager. Esto garantiza que el CloudWatch el agente se mantiene actualizado y puede informar y corregir los servidores que no tienen CloudWatch agente. Este enfoque también se amplía para admitir varias cuentas y regiones.
- Implementación del CloudWatch agente como parte del script de datos de usuario durante el aprovisionamiento de instancias de EC2— Amazon EC2 le permite definir un script de inicio que se ejecuta cuando arranca o reinicia por primera vez. Puede definir un script para automatizar el proceso de descarga e instalación del agente. Esto también se puede incluir enAWS CloudFormationscripts yAWSProductos de Service Catalog. Este enfoque podría ser apropiado según sea necesario si existe un enfoque de instalación y configuración de agente personalizado para una carga de trabajo específica que se desvía de los estándares.
- Inclusión del agente de CloudWatch en Amazon Machine Images (AMI)— Puede instalar el agente de CloudWatch en sus AMI personalizadas para Amazon EC2. Las instancias EC2 que utilizan la AMI tendrán el agente instalado y se iniciará automáticamente. Sin embargo, debe asegurarse de que el agente y su configuración se actualizan periódicamente.

Instalación de CloudWatch agente mediante el Systems Manager Distributor y State Manager

Puede utilizar Systems Manager State Manager con Systems Manager Distributor para instalar y actualizar automáticamente el CloudWatch agente en servidores e instancias EC2. El distribuidor incluye el`AmazonCloudWatchAgent` AWSpaquete administrado que instala la versión del agente de CloudWatch más reciente.

Este enfoque de instalación tiene los requisitos previos siguientes:

- El agente de Systems Manager debe estar instalado y en ejecución en sus servidores o instancias EC2. El agente de Systems Manager está preinstalado en Amazon Linux, Amazon Linux 2 y algunas AMI. El agente también debe instalarse y configurarse en otras imágenes o máquinas virtuales y servidores locales.
- Un rol o credenciales de IAM que tienen el: obligatorio CloudWatch permisos de Systems Managerdebe estar asociado a la instancia EC2 o definido en el archivo de credenciales de un servidor local. Por ejemplo, puede crear un rol de IAM que incluya elAWSpolíticas administradas:`AmazonSSMManagedInstanceCore`para Systems Manager y`CloudWatchAgentServerPolicy`para CloudWatch. Puede utilizar elssm-cloudwatch-instance-role.yaml AWS CloudFormationplantilla para implementar un rol de IAM y un perfil de instancia que incluye ambas políticas. Esta plantilla también se puede modificar para incluir otros permisos de IAM estándar para las instancias EC2. Para servidores locales o máquinas virtuales, debe configurar la CloudWatch agente de para utilizar elFunción de servicio de Systems Managerque se configuró para el servidor local. Para obtener más información acerca de este tema, consulte¿Cómo puedo configurar servidores locales que utilizan Systems Manager Agent y el sistema unificado? CloudWatch agente para usar solo credenciales temporales?en laAWSCentro de conocimiento.

La lista siguiente ofrece varias ventajas para utilizar el enfoque Distributor de Systems Manager y State Manager para instalar y mantener el CloudWatch agente:

- Instalación automatizada para varios sistemas operativos: no necesita escribir ni mantener un script para cada SO para descargar e instalar el agente de CloudWatch.
- Verificaciones automáticas de actualizaciones— State Manager comprueba de forma automática y periódica que cada instancia de EC2 tiene la versión más reciente de CloudWatch.
- Informes de cumplimiento— El panel de conformidad de Systems Manager muestra qué instancias de EC2 no han podido instalar correctamente el paquete Distributor.
- Instalación automatizada para instancias EC2 lanzadas recientemente— Las nuevas instancias EC2 que se lanzan en su cuenta reciben automáticamente el CloudWatch agente.

Sin embargo, también debe tener en cuenta las tres áreas siguientes antes de elegir este enfoque:

- Colisión con una asociación existente— Si otra asociación ya instala o configura el CloudWatch agente, entonces las dos asociaciones podrían interferir entre sí y provocar problemas. Al utilizar

este enfoque, debe eliminar cualquier asociación existente que instale o actualice el agente y la configuración de CloudWatch.

- Actualización de archivos de configuración de agente personalizados— El distribuidor realiza una instalación mediante el archivo de configuración predeterminado. Si utiliza un archivo de configuración personalizado o varios CloudWatch archivos de configuración, debe actualizar la configuración después de la instalación.
- Configuración de varias regiones o cuentas múltiples— La asociación de gestores estatales debe configurarse en cada cuenta y región. Las cuentas nuevas en un entorno de varias cuentas deben actualizarse para incluir la asociación State Manager. Necesita centralizar o sincronizar el CloudWatch configuración para que varias cuentas y regiones puedan recuperar y aplicar los estándares requeridos.

Configurar State Manager y distribuidor para CloudWatch implementación y configuración de agentes

Puede usarConfiguración rápida de Systems Managerpara configurar rápidamente las funciones de Systems Manager, incluida la instalación y actualización automáticas del CloudWatch agente en sus instancias EC2. La configuración rápida implementa unAWS CloudFormationpila que implementa y configura los recursos de Systems Manager en función de sus elecciones.

En la lista siguiente se proporcionan dos acciones importantes que realiza la configuración rápida para automatizar CloudWatch instalación y actualización del agente:

1. Creación de documentos personalizados de Systems Manager— La configuración rápida crea los siguientes documentos de Systems Manager para utilizarlos con State Manager. Los nombres de los documentos pueden variar, pero el contenido sigue siendo el mismo:
   - `CreateAndAttachIAMToInstance`— Crea el`AmazonSSMRoleForInstancesQuickSetup`perfil de rol e instancia si no existen y adjunta el`AmazonSSMManagedInstanceCore`política de para el rol. Esto no incluye el requerido`CloudWatchAgentServerPolicy`Política de IAM. Debe actualizar esta política y actualizar este documento de Systems Manager para incluir esta política tal y como se describe en la siguiente sección.
   - `InstallAndManageCloudWatchDocument`— Instala el CloudWatch agente con Distributor y configura cada instancia de EC2 una vez con un valor predeterminado CloudWatch

configuración del agente mediante elAWS-ConfigureAWSPackageDocumento de Systems Manager.

- UpdateCloudWatchDocument— Actualizar el CloudWatch agente mediante la instalación del último agente de CloudWatch mediante elAWS-ConfigureAWSPackageDocumento de Systems Manager. Actualizar o desinstalar el agente no elimina el existente CloudWatch archivos de configuración de la instancia EC2.

2. Crear asociaciones de State Manager— Las asociaciones de State Manager se crean y configuran para utilizar los documentos de Systems Manager creados personalizados. Los nombres de asociación de State Manager pueden variar, pero la configuración sigue siendo la misma:
   - ManageCloudWatchAgent— Ejecute laInstallAndManageCloudWatchDocumentDocumentar Systems Manager una vez para cada instancia de EC2.
   - UpdateCloudWatchAgent— Ejecute laUpdateCloudWatchDocumentDocumento de Systems Manager cada 30 días para cada instancia de EC2.
   - Ejecute laCreateAndAttachIAMToInstanceDocumentar Systems Manager una vez para cada instancia de EC2.

Debe aumentar y personalizar la configuración de configuración rápida completada para incluir permisos de CloudWatch y soporte personalizado CloudWatch configuraciones. En particular, elCreateAndAttachIAMToInstancey laInstallAndManageCloudWatchDocumentdeberá actualizarse el documento. Puede actualizar manualmente los documentos de Systems Manager creados por la configuración rápida. También puede utilizar el suyo propio CloudFormation para aprovisionar los mismos recursos con las actualizaciones necesarias, así como configurar e implementar otros recursos de Systems Manager y no utilizar la configuración rápida.

> **Important**
>
> La instalación rápida crea unAWS CloudFormationpila para implementar y configurar los recursos de Systems Manager en función de sus elecciones. Si actualiza las opciones de configuración rápida, es posible que tenga que volver a actualizar manualmente los documentos de Systems Manager.

En las siguientes secciones se describe cómo actualizar manualmente los recursos de Systems Manager creados por la instalación rápida, así como utilizar los suyos propios.AWS

CloudFormationplantilla para realizar una configuración rápida actualizada. Le recomendamos que utilice el suyo propioAWS CloudFormationplantilla para evitar actualizar manualmente los recursos creados por la configuración rápida yAWS CloudFormation.

Utilice la configuración rápida de Systems Manager y actualice manualmente los recursos creados de Systems Manager

Los recursos de Systems Manager creados por el enfoque de configuración rápida deben actualizarse para incluir lo necesario CloudWatch permisos de agente y soporte múltiple CloudWatch archivos de configuración. En esta sección se describe cómo actualizar el rol de IAM y los documentos de Systems Manager para utilizar un bucket de S3 centralizado que contiene CloudWatch configuraciones a las que se puede acceder desde varias cuentas. Creación de un bucket de S3 para almacenar el CloudWatch Los archivos de configuración se describen en elAdministrar CloudWatch las configuracionessección de esta guía.

Actualizar el**`CreateAndAttachIAMToInstance`**Documento de Systems Manager

Este documento de Systems Manager creado por Quick Setup comprueba si una instancia EC2 tiene adjunto un perfil de instancia de IAM existente. Si lo hace, adjunta el`AmazonSSMManagedInstanceCore`política de la función existente. Esto protege las instancias EC2 existentes de que no se pierdan.AWSpermisos que se pueden asignar a través de perfiles de instancias existentes. Debe agregar un paso en este documento para adjuntar el`CloudWatchAgentServerPolicy`Política de IAM para instancias EC2 que ya tienen un perfil de instancia adjunto. El documento de Systems Manager también crea el rol de IAM si no existe y una instancia de EC2 no tiene un perfil de instancia adjunto a él. Debe actualizar esta sección del documento para incluir también el`CloudWatchAgentServerPolicy`Política de IAM.

Realice la revisión delCrear y adjuntar IAM a instancia.yamldocumento de ejemplo y compárelo con el documento creado por la instalación rápida. Edite el documento existente para incluir los pasos y cambios necesarios. En función de las opciones de configuración rápida, el documento creado por la Configuración rápida puede ser diferente del documento de ejemplo proporcionado, así que asegúrese de realizar los ajustes necesarios. El documento de ejemplo incluye la opción de configuración rápida para analizar las instancias en busca de parches que faltan diariamente y, por lo tanto, incluye una política para Systems Manager Patch Manager.

Actualizar el**`InstallAndManageCloudWatchDocument`**Documento de Systems Manager

Este documento de Systems Manager creado por Quick Setup instala el CloudWatch agente y lo configura con el valor predeterminado CloudWatch configuración del agente de. El valor de tiempo de espera predeterminado de CloudWatch configuración se alinea con el conjunto de métricas básico predefinido. Debe reemplazar el paso de configuración predeterminado y agregar pasos para descargar su CloudWatch archivos de configuración de su CloudWatch bucket de configuración de S3.

Realice la revisión delInstalación y administración de CloudWatchDocument.yamldocumento actualizado y compararlo con el documento creado por la instalación rápida. El documento creado por la Configuración rápida puede ser diferente, así que asegúrese de haber realizado los ajustes necesarios. Edite el documento existente para incluir los pasos y cambios necesarios.

UsarAWS CloudFormationen lugar de Configuración rápida

En lugar de utilizar la configuración rápida de, puede utilizarAWS CloudFormationpara configurar Systems Manager. Este enfoque le permite personalizar la configuración de Systems Manager de acuerdo a sus requisitos específicos. Este enfoque también evita las actualizaciones manuales de los recursos configurados de Systems Manager creados por la configuración rápida para admitir la personalización CloudWatch configuraciones.

La función Configuración rápida también utilizaAWS CloudFormationy crea unAWS CloudFormationconjunto de pilas para implementar y configurar los recursos de Systems Manager en función de sus elecciones. Antes de poder usarAWS CloudFormationconjuntos de pila, debe crear los roles de IAM utilizados porAWS CloudFormation StackSets para admitir implementaciones en varias cuentas o regiones. La configuración rápida crea las funciones que necesita para admitir implementaciones de varias regiones o cuentas conAWS CloudFormationStackSets. Debe completar los requisitos previos paraAWS CloudFormation StackSets si desea configurar e implementar recursos de Systems Manager en varias regiones o en varias cuentas desde una única cuenta y región. Para obtener más información acerca de este tema, consulteRequisitos previos para las operaciones con conjuntos de pilasen laAWS CloudFormation.

Consulte elConfiguración rápida de AWS - SSM Hostmgmt.yaml AWS CloudFormationplantilla para la configuración rápida personalizada.

Debe revisar los recursos y las capacidades delAWS CloudFormationplantilla y haga ajustes de acuerdo a sus necesidades. Debería controlar la versiónAWS CloudFormationplantilla que utiliza

y prueba los cambios de forma incremental para confirmar el resultado requerido. Además, debe realizar revisiones de seguridad en la nube para determinar si se requieren ajustes de política en función de los requisitos de su organización.

Debería implementar elAWS CloudFormationapilar en una única cuenta de prueba y región, y realizar los casos de prueba necesarios para personalizar y confirmar el resultado deseado. A continuación, puede graduar la implementación en varias regiones en una sola cuenta y, a continuación, en varias cuentas y varias regiones.

Configuración rápida personalizada en una única cuenta y región conAWS CloudFormationpila

Si solo utiliza una cuenta y una región, puede implementar el ejemplo completo comoAWS CloudFormationpila en lugar de unaAWS CloudFormationconjunto de pilas. Sin embargo, si es posible, le recomendamos que utilice el enfoque de conjuntos de pilas multirregión y varias cuentas, aunque solo use una sola cuenta y una región. Uso deAWS CloudFormation StackSets facilita la ampliación a cuentas y regiones adicionales en el future.

Siga los pasos a continuación para implementar elConfiguración rápida de AWS - SSM Hostmgmt.yaml AWS CloudFormationplantilla comoAWS CloudFormationpila en una sola cuenta y región:

1. Descargue la plantilla y compruebe su sistema de control de versiones preferido (por ejemplo,AWS CodeCommit).
2. Personalizar el valor predeterminadoAWS CloudFormationvalores de parámetros basados en los requisitos de su organización.
3. Personalizar los programas de asociaciones de State Manager.
4. Personalizar el documento de Systems Manager con el`InstallAndManageCloudWatchDocument`ID lógico. Confirme que los prefijos de bucket de S3 se alinean con los prefijos del bucket de S3 que contiene su CloudWatch Configuración de .
5. Recupere y registre el nombre de recurso de Amazon (ARN) del bucket de S3 que contiene su CloudWatch configuraciones. Para obtener más información acerca de este tema, consulte laAdministrar CloudWatch las configuracionessección de esta guía. Una muestracloudwatch-config-s3-bucket.yaml AWS CloudFormationestá disponible una plantilla que incluye una política de bucket para proporcionar acceso de lectura aAWS Organizationscuentas.
6. Implementación de la configuración rápida personalizadaAWS CloudFormationplantilla en la misma cuenta que su bucket de S3:

- Para el registro`CloudWatchConfigBucketARN`introduzca el ARN del bucket de S3.
- Realice ajustes en las opciones de parámetros en función de las capacidades que desee habilitar para Systems Manager.

7. Implemente una instancia EC2 de prueba con y sin un rol de IAM para confirmar que la instancia EC2 funciona con CloudWatch.

- Aplicar el`AttachIAMToInstance`Asociación de State Manager. Se trata de un runbook de Systems Manager que está configurado para ejecutarse de acuerdo con una programación. Las asociaciones de State Manager que utilizan runbooks no se aplican automáticamente a las nuevas instancias de EC2 y se pueden configurar para que se ejecuten de forma programada. Para obtener más información, consulteEjecución de automatizaciones con desencadenadores mediante el State Manageren la documentación de Systems Manager.
- Confirme que la instancia EC2 tiene adjunta la función de IAM requerida.
- Confirme que el agente de Systems Manager funciona correctamente confirmando que la instancia EC2 está visible en Systems Manager.
- Confirme que el CloudWatch agente funciona correctamente mediante la visualización CloudWatch registros y métricas basados en el CloudWatch configuraciones de su bucket de S3.

Configuración rápida personalizada en varias regiones y varias cuentas conAWS CloudFormationConjuntos de pilas

Si utiliza varias cuentas y regiones, puede implementar laConfiguración rápida de AWS - SSM Hostmgmt.yaml AWS CloudFormationplantilla como conjunto de pila. Debe completar elAWS CloudFormationRequisitos previos de StackSetantes de usar conjuntos de pila. Los requisitos varían según si va a implementar conjuntos de pila conautoadministradooservicio administradoPermisos de.

Le recomendamos que implemente conjuntos de pilas con permisos administrados por servicios para que las nuevas cuentas reciban automáticamente la configuración rápida personalizada. Debe implementar un conjunto de pilas administrados por servicio desde elAWS Organizationscuenta de administración o cuenta de administrador delegada. Debe implementar el conjunto de pilas desde una cuenta centralizada utilizada para la automatización que tiene privilegios de administrador delegados, en lugar de laAWS Organizationscuenta de administración. También le recomendamos que pruebe la implementación del conjunto de pilas dirigiéndose a una unidad organizativa (OU) de prueba con un número único o pequeño de cuentas en una región.

1. Complete los pasos 1 a 5 desde elConfiguración rápida personalizada en una única cuenta y región conAWS CloudFormationpilasección de esta guía.
2. Inicie sesión en elAWS Management Console, abra elAWS CloudFormationconsolador y eligeCrear StackSet:
   - ElegirTemplate is ready (La plantilla está lista)yUpload a template file (Cargar un archivo de plantilla). Cargar elAWS CloudFormationplantilla que ha personalizado según sus necesidades.
   - Especifique los detalles del conjunto de pilas:
     - Introduzca un nombre de conjunto de pila, por ejemplo,`StackSet-SSM-QuickSetup`.
     - Realice ajustes en las opciones de parámetros en función de las capacidades que desee habilitar para Systems Manager.
     - Para el registro`CloudWatchConfigBucketARN`, escriba el ARN de su CloudWatch bucket de la configuración de S3.
     - Especifique las opciones del conjunto de pilas y elija si utilizará permisos administrados por servicios conAWS Organizationso permisos autoadministrados.
       - Si elige permisos autogestionados, introduzca laFunción de administración de AWS Cloud Formation StacksetyFunción de ejecución de AWS Cloud Formation StacksetDetalles del rol de IAM. El rol de administrador debe existir en la cuenta y el rol de ejecución debe existir en cada cuenta de destino
     - Paraservicio administradopermisos conAWS Organizations, le recomendamos que primero lo implemente en una unidad organizativa de prueba en lugar de en toda la organización.
       - Elija si desea habilitar las implementaciones automáticas. Le recomendamos que elijaEnabled (Habilitado). Para el comportamiento de eliminación de cuentas, la configuración recomendada esEliminar pilas.
     - Paraautoadministradopermisos, introduzca laAWSID de cuenta de las cuentas que desea configurar. Debe repetir este proceso para cada nueva cuenta si utiliza permisos autogestionados.
     - Introduzca las regiones en las que va a utilizar CloudWatch y Systems Manager.
     - Para confirmar que la implementación se ha realizado correctamente, consulte el estado en elOperaciones yInstancias de pilapestaña para el conjunto de pilas.
     - Pruebe que Systems Manager y CloudWatch funcionan correctamente en las cuentas implementadas siguiendo el paso 7 de laConfiguración rápida personalizada en una única cuenta y región conAWS CloudFormationpilasección de esta guía.

Consideraciones para configurar servidores en las instalaciones

La CloudWatch agente para servidores y máquinas virtuales locales se instala y configura mediante un enfoque similar al de las instancias EC2. Sin embargo, en la siguiente tabla se proporcionan consideraciones que debe evaluar al instalar y configurar el CloudWatch agente en servidores locales y máquinas virtuales.

Apunte la CloudWatch agente con las mismas credenciales temporales utilizadas para Systems Manager.	Cuando configura Systems Manager en un entorno híbrido que incluye servidores locales, puede activar Systems Manager con un rol de IAM. Debe utilizar el rol creado para las instancias EC2 que incluye el`CloudWatchAgentServerPolicy` y`AmazonSSMManagedInstanceCore` políticas. Esto hace que el agente de Systems Manager recupere y escriba credenciales temporales en un archivo de credenciales local. Puedes apuntar tu CloudWatch configuración del agente en el mismo archivo. Puede utilizar el proceso desdeConfigurar servidores locales que utilizan el agente de Systems Manager y el agente de CloudWatch unificado para utilizar solo credenciales temporalesen laAWSCentro de conocimiento. También puede automatizar este proceso definiendo un runbook de Systems Manager Automation y una asociación de State Manager independientes, y segmentando las instancias locales con etiquetas. Al crear unActivación de Systems Managerpara las instancias locales, debe incluir una etiqueta que identifique las instancias como instancias locales.

Considere utilizar cuentas y regiones que tengan VPN oAWS Direct Connectacceso a yAWSPrivateLink.	Puede usarAWS Direct ConnectoAWS Virtual Private Network(AWS VPN) para establecer conexiones privadas entre las redes locales y su nube virtual privada (VPC).AWS PrivateLink establece una conexión privada a CloudWatc h Registros con un punto de enlace de la VPC de tipo interfaz. Este enfoque resulta útil si tiene restricciones que impiden que los datos se envíen a través de Internet pública a un endpoint de servicio público.
Todas las métricas deben incluirse en el CloudWatch archivo de configuración.	Amazon EC2 incluye métricas estándar (por ejemplo, utilización de CPU) pero estas métricas deben definirse para las instancias locales. Puede utilizar un archivo de configura ción de plataforma independiente para definir estas métricas para los servidores locales y, a continuación, agregar la configuración al estándar CloudWatch configuración de métricas para la plataforma.

Consideraciones para instancias EC2 efímeras

Las instancias EC2 son temporales, oefímero, si Amazon EC2 Auto Scaling, Amazon EMR,Instancias de spot de Amazon EC2, o bienAWS Batch. Las instancias EC2 efímeras pueden provocar un gran número de CloudWatch transmisiones en un grupo de registros común sin información adicional sobre su origen en tiempo de ejecución.

Si utiliza instancias EC2 efímeras, considere la posibilidad de agregar información contextual dinámica adicional en el grupo de registros y los nombres de las secuencias de registros. Por ejemplo, puede incluir el ID de solicitud de instancia de spot, el nombre del clúster de Amazon EMR o el nombre del grupo de Auto Scaling. Esta información puede variar para las instancias EC2 recién lanzadas y es posible que tenga que recuperarla y configurarla en tiempo de ejecución. Para hacerlo, escriba un CloudWatch archivo de configuración del agente al arrancar y reiniciar el agente para incluir el archivo de configuración actualizado. Esto permite la entrega de registros y métricas a CloudWatch mediante información dinámica en tiempo de ejecución.

También debes asegurarte de que las métricas y los registros se envían mediante el CloudWatch agente antes de que finalicen las instancias EC2 efímeras. La CloudWatch agente incluye `unflush_interval`parámetro que se puede configurar para definir el intervalo de tiempo para vaciar búferes de registro y métricas. Puede reducir este valor en función de su carga de trabajo y detener el CloudWatch y forzar el vaciado de los búferes antes de que finalice la instancia EC2.

Uso de una solución automatizada para implementar el CloudWatch agente

Si utiliza una solución de automatización (por ejemplo, Ansible o Chef), puede aprovecharla para instalar y actualizar automáticamente el CloudWatch agente. Si utiliza este enfoque, debe evaluar las siguientes consideraciones:

- Valide que la automatización cubra los sistemas operativos y las versiones del SO compatibles. Si el script de automatización no es compatible con todos los sistemas operativos de su organización, debe definir soluciones alternativas para los sistemas operativos no compatibles.
- Valide que la solución de automatización compruebe periódicamente las actualizaciones y actualizaciones de los agentes de CloudWatch. Su solución de automatización debería comprobar periódicamente si hay actualizaciones en el CloudWatch o desinstale y vuelva a instalar regularmente el agente. Puede utilizar un programador o una funcionalidad de solución de automatización para comprobar y actualizar periódicamente el agente.
- Valide que puede confirmar la instalación del agente y el cumplimiento de la configuración. La solución de automatización debería permitirle determinar cuándo un sistema no tiene instalado el agente o cuándo el agente no funciona. Puede implementar una notificación o alarma en la solución de automatización para que se realice un seguimiento de las instalaciones y configuraciones fallidas.

Implementación del CloudWatch agente durante el aprovisionamiento de instancias con el script de datos de usuario

Puede utilizar este enfoque si no planea utilizar Systems Manager y desea utilizar CloudWatch de forma selectiva para sus instancias EC2. Normalmente, este enfoque se utiliza una sola vez o cuando se requiere una configuración especializada.AWSproporcionaenlaces directospara la CloudWatch agente que se puede descargar en los scripts de datos de inicio o de usuario. Los paquetes de instalación del agente se pueden ejecutar de forma silenciosa sin interacción del usuario, lo que significa que puede utilizarlos en implementaciones automatizadas. Si utiliza este enfoque, debe evaluar las siguientes consideraciones:

- Mayor riesgo de que los usuarios no instalen el agente ni configuren métricas estándar. Los usuarios pueden aprovisionar instancias sin incluir los pasos necesarios para instalar el CloudWatch agente. También podrían configurar mal el agente, lo que podría provocar incoherencias de registro y supervisión.
- Los scripts de instalación deben ser específicos del sistema operativo y ser adecuados para diferentes versiones del SO. Necesita secuencias de comandos independientes si pretendía utilizar Windows y Linux. El script de Linux también debe tener diferentes pasos de instalación según la distribución.
- Debe actualizar periódicamente el CloudWatch agente con nuevas versiones cuando esté disponible. Esto se puede automatizar si utiliza Systems Manager con State Manager, pero también puede configurar el script de datos de usuario para que se vuelva a ejecutar al iniciar la instancia. La CloudWatch el agente se actualiza y se vuelve a instalar en cada reinicio.
- Debe automatizar la recuperación y la aplicación de las configuraciones estándar de CloudWatch. Esto se puede automatizar si utiliza Systems Manager con State Manager, pero también puede configurar un script de datos de usuario para recuperar los archivos de configuración al arrancar y reiniciar el CloudWatch agente.

Inclusión del CloudWatch agente en tus AMI

La ventaja de utilizar este enfoque es que no tiene que esperar a que CloudWatch agente que se va a instalar y configurar, y puede comenzar inmediatamente a registrar y supervisar. Esto le ayuda a supervisar mejor los pasos de inicio y aprovisionamiento de instancias en caso de que las instancias no se inicien. Este enfoque también es adecuado si no planea utilizar el agente de Systems Manager. Si utiliza este enfoque, debe evaluar las siguientes consideraciones:

- Debe existir un proceso de actualización porque es posible que las AMI no incluyan las más recientes CloudWatch Versión del agente de. La CloudWatch agente instalado en una AMI solo está actualizado hasta la última vez que se creó la AMI. Debe incluir un método adicional para actualizar el agente periódicamente y cuando se aprovisione la instancia EC2. Si utiliza Systems Manager, puede utilizar elInstalación de CloudWatch agente mediante el Systems Manager Distributor y State Managersolución que se proporciona en esta guía para ello. Si no utiliza Systems Manager, puede utilizar un script de datos de usuario para actualizar el agente al iniciar y reiniciar la instancia.

- Sus CloudWatch el archivo de configuración del agente debe recuperarse al iniciar la instancia. Si no utiliza Systems Manager, puede configurar un script de datos de usuario para recuperar los archivos de configuración al arrancar y, a continuación, reiniciar el CloudWatch agente.
- La CloudWatch el agente debe reiniciarse después de que su CloudWatch La configuración se actualiza.
- AWSlas credenciales no deben guardarse en la AMI. Asegúrese de que no hay localesAWSLas credenciales se guardan en la AMI. Si utiliza Amazon EC2, puede aplicar el rol de IAM necesario a la instancia y evitar credenciales locales. Si utiliza instancias locales, debe automatizar o actualizar manualmente las credenciales de la instancia antes de iniciar el CloudWatch agente.

Registro y supervisión en Amazon ECS

Amazon Elastic Container Service (Amazon ECS) proporciona dos tipos de lanzamiento para los contenedores en ejecución y que determinan el tipo de infraestructura que aloja las tareas y los servicios; estos tipos de lanzamiento AWS Fargate son Amazon EC2. Ambos tipos de lanzamiento se integran CloudWatch , pero las configuraciones y el soporte varían.

Las siguientes secciones le ayudan a entender cómo utilizarlas CloudWatch para el registro y la supervisión en Amazon ECS.

Temas

Configuración CloudWatch con un tipo de lanzamiento de EC2

Con un tipo de lanzamiento de EC2, aprovisiona un clúster de Amazon ECS de instancias EC2 que utilizan el CloudWatch agente para el registro y la supervisión. Una AMI optimizada para Amazon ECS viene preinstalada con el agente contenedor de Amazon ECS y proporciona CloudWatch métricas para el clúster de Amazon ECS.

Estas métricas predeterminadas se incluyen en el coste de Amazon ECS, pero la configuración predeterminada de Amazon ECS no supervisa los archivos de registro ni las métricas adicionales (por ejemplo, el espacio libre en disco). Puede usarlo AWS Management Console para aprovisionar un clúster de Amazon ECS con el tipo de lanzamiento EC2, lo que crea una AWS CloudFormation pila que despliega un Amazon EC2 Auto Scaling grupo con una configuración de lanzamiento. Sin embargo, este enfoque significa que no puede elegir una AMI personalizada ni personalizar la configuración de inicio con ajustes diferentes o scripts de arranque adicionales.

Para monitorear registros y métricas adicionales, debe instalar el CloudWatch agente en sus instancias de contenedor de Amazon ECS. Puede utilizar el enfoque de instalación para las instancias EC2 de la Instalación de CloudWatch agente mediante el Systems Manager Distributor y State Manager sección de esta guía. Sin embargo, la AMI de Amazon ECS no incluye el agente de Systems Manager necesario. Debe utilizar una configuración de lanzamiento personalizada con un

script de datos de usuario que instale el agente de Systems Manager al crear el clúster de Amazon ECS. Esto permite que las instancias de contenedor se registren en Systems Manager y apliquen las asociaciones de State Manager para instalar, configurar y actualizar el CloudWatch agente. Cuando State Manager ejecuta y actualiza la configuración del CloudWatch agente, también aplica la configuración estandarizada a nivel de sistema para CloudWatch Amazon EC2. También puede almacenar CloudWatch las configuraciones estandarizadas de Amazon ECS en el bucket de S3 para su CloudWatch configuración y aplicarlas automáticamente con State Manager.

Debe asegurarse de que el perfil de instancia o rol de IAM aplicado a sus instancias de contenedor de Amazon ECS incluya las `AmazonSSMManagedInstanceCore` políticas `CloudWatchAgentServerPolicy` y los requisitos. Puede usar la plantilla ecs_cluster_with_cloudwatch_linux.yaml para AWS CloudFormation aprovisionar clústeres Amazon ECS basados en Linux. Esta plantilla crea un clúster de Amazon ECS con una configuración de lanzamiento personalizada que instala Systems Manager e implementa una CloudWatch configuración personalizada para supervisar los archivos de registro específicos de Amazon ECS.

Debe capturar los siguientes registros para sus instancias de contenedor de Amazon ECS, así como los registros de instancias EC2 estándar:

- Resultado de inicio del agente Amazon ECS — `/var/log/ecs/ecs-init.log`
- Salida del agente Amazon ECS — `/var/log/ecs/ecs-agent.log`
- Registro de solicitudes del proveedor de credenciales de IAM — `/var/log/ecs/audit.log`

Para obtener más información sobre el nivel de salida, el formato y las opciones de configuración adicionales, consulte las ubicaciones de los archivos de registro de Amazon ECS en la documentación de Amazon ECS.

> **Important**
>
> No se requiere la instalación o configuración del agente para el tipo de lanzamiento de Fargate porque no se ejecutan ni administran instancias de contenedor de EC2.

Las instancias de contenedor de Amazon ECS deben usar las AMI y el agente de contenedor más recientes optimizados para Amazon ECS. AWS almacena los parámetros públicos del almacén de parámetros de Systems Manager con información de AMI optimizada para Amazon ECS, incluida la ID de la AMI. Puede recuperar la última AMI optimizada más recientemente del almacén de

parámetros mediante el formato de parámetros del almacén de parámetros para las AMI optimizadas para Amazon ECS. Puede hacer referencia al parámetro público del almacén de parámetros que hace referencia a la AMI más reciente o a una versión específica de la AMI en sus AWS CloudFormation plantillas.

AWS proporciona los mismos parámetros del almacén de parámetros en cada región compatible. Esto significa que AWS CloudFormation las plantillas que hacen referencia a estos parámetros se pueden reutilizar en todas las regiones y cuentas sin necesidad de actualizar la AMI. Puede controlar la implementación de las AMI de Amazon ECS más nuevas en su organización consultando una versión específica, lo que le ayuda a evitar el uso de una nueva AMI optimizada para Amazon ECS hasta que la pruebe.

Registros de contenedores de Amazon ECS para los tipos de lanzamiento de EC2 y Fargate

Amazon ECS utiliza una definición de tareas para implementar y gestionar contenedores como tareas y servicios. Usted configura los contenedores que quiere lanzar en su clúster de Amazon ECS dentro de una definición de tarea. El registro se configura con un controlador de registro a nivel de contenedor. Las múltiples opciones de controladores de registro proporcionan a sus contenedores diferentes sistemas de registro (por ejemplo `awslogs`,`fluentd`,`gelf`,`json-file`,`journald`,`logentries`, `splunk`, o`syslog`,`awsfirelens`) en función de si utiliza el tipo de lanzamiento EC2 o Fargate. El tipo de lanzamiento Fargate proporciona un subconjunto de las siguientes opciones de controladores de registro:`awslogs`, `splunk`. `awsfirelens` AWS proporciona el controlador de `awslogs` registro para capturar y transmitir la salida del contenedor a CloudWatch Logs. La configuración del controlador de registro le permite personalizar el grupo de registros, la región y el prefijo del flujo de registro, junto con muchas otras opciones.

El nombre predeterminado de los grupos de registros y la opción utilizada en la opción de configuración automática de CloudWatch registros son. AWS Management Console `/ecs/<task_name>` El nombre del flujo de registro utilizado por Amazon ECS tiene este `<awslogs-stream-prefix>/<container_name>/<task_id>` formato. Le recomendamos que utilice un nombre de grupo que agrupe sus registros en función de los requisitos de su organización. En la siguiente tabla, los `image_name` y `image_tag` se incluyen en el nombre del flujo de registro.

Nombre del grupo de registros	`/<Business unit>/<Project or application name>/<Environment>/<Cluster name>/<Task name>`
Prefijo del nombre del flujo de registro	`/<image_name>/<image_tag>`

Esta información también está disponible en la definición de la tarea. Sin embargo, las tareas se actualizan periódicamente con nuevas revisiones, lo que significa que la definición de la tarea puede haber utilizado un `image_name` Y `image_tag` diferente al que utiliza actualmente la definición de la tarea. Para obtener más información y sugerencias de nombres, consulte la Planificación de la CloudWatch implementación sección de esta guía.

Si utilizas una canalización de integración y entrega continuas (CI/CD) o un proceso automatizado, puedes crear una nueva revisión de la definición de tareas para tu aplicación con cada nueva creación de imagen de Docker. Por ejemplo, puede incluir el nombre de la imagen de Docker, la etiqueta de la imagen, la GitHub revisión u otra información importante en la configuración de registro y revisión de la definición de la tarea como parte del proceso de CI/CD.

Uso del enrutamiento de registros personalizado con FireLens Amazon ECS

FireLens para Amazon ECS le ayuda a enrutar los registros a Fluentd o Fluent Bit para que pueda enviar directamente los registros de contenedores a los AWS servicios y a los destinos de la red de AWS socios (APN), además de admitir el envío de registros a Logs. CloudWatch

AWS proporciona una imagen de Docker para Fluent Bit con complementos preinstalados para Amazon Kinesis Data Streams, Amazon Data Firehose y Logs. CloudWatch Puede utilizar el controlador de FireLens registro en lugar del controlador de `awslogs` registro para personalizar y controlar mejor los registros enviados a Logs. CloudWatch

Por ejemplo, puede usar el controlador de FireLens registro para controlar la salida del formato de registro. Esto significa que los CloudWatch registros de un contenedor de Amazon ECS se formatean automáticamente como objetos JSON e incluyen propiedades con formato JSON para`ecs_cluster`,, `ecs_task_arn``ecs_task_definition`, `container_id` y. `container_name` `ec2_instance_id` El host fluido queda expuesto a su contenedor a través de las variables de `FLUENT_PORT` entorno `FLUENT_HOST` y cuando usted especifica el controlador.

`awsfirelens` Esto significa que puedes iniciar sesión directamente en el router de registros desde tu código mediante bibliotecas de registro fluidas. Por ejemplo, su aplicación podría incluir la `fluent-logger-python` biblioteca para iniciar sesión en Fluent Bit utilizando los valores disponibles en las variables de entorno.

Si decide usarlo FireLens para Amazon ECS, puede configurar los mismos ajustes que el controlador de `awslogs` registro y usar también otros ajustes. Por ejemplo, puede usar la definición de tarea de Amazon ECS ecs-task-nginx-firelense.json que lanza un servidor NGINX configurado FireLens para usarse para iniciar sesión en. CloudWatch También lanza un contenedor FireLens Fluent Bit como sidecar para el registro.

Métricas de Amazon ECS

Amazon ECS proporciona CloudWatch métricas estándar (por ejemplo, el uso de la CPU y la memoria) para los tipos de lanzamiento de EC2 y Fargate a nivel de clúster y servicio con el agente contenedor de Amazon ECS. También puede capturar métricas para sus servicios, tareas y contenedores mediante CloudWatch Container Insights, o capturar sus propias métricas de contenedores personalizadas mediante el formato de métricas integrado.

Container Insights es una CloudWatch función que proporciona métricas como la utilización de la CPU, la utilización de la memoria, el tráfico de red y el almacenamiento a nivel de clúster, instancia de contenedor, servicio y tarea. Container Insights también crea paneles automáticos que le ayudan a analizar los servicios y las tareas y a ver el uso medio de la memoria o la CPU a nivel de contenedor. Container Insights publica métricas personalizadas en el espacio de nombres `ECS/ContainerInsights` personalizado que puedes usar para crear gráficos, generar alarmas y crear paneles.

Puede activar las métricas de Container Insight habilitando Container Insights para cada clúster individual de Amazon ECS. Si también quiere ver las métricas a nivel de instancia de contenedor, puede lanzar el CloudWatch agente como un contenedor daemon en su clúster de Amazon ECS. Puede usar la AWS CloudFormation plantilla cwagent-ecs-instance-metric-cfn.yaml para implementar el agente CloudWatch como un servicio de Amazon ECS. Es importante destacar que en este ejemplo se supone que creó una configuración de CloudWatch agente personalizada adecuada y la almacenó en el almacén de parámetros con la clave. `ecs-cwagent-daemon-service`

El CloudWatchagente desplegado como contenedor daemon para CloudWatch Container Insights incluye métricas adicionales de disco, memoria y CPU, como las `InstanceId`

dimensiones `ClusterNameContainerInstanceId`, `instance_cpu_reserved_capacity` y `instance_memory_reserved_capacity` con ellas. Container Insights implementa las métricas a nivel de instancia de contenedor mediante el formato de métricas CloudWatch integrado. Puede configurar métricas adicionales a nivel de sistema para sus instancias de contenedor de Amazon ECS mediante el enfoque de la Configurar State Manager y distribuidor para CloudWatch implementación y configuración de agentes sección de esta guía.

Creación de métricas de aplicaciones personalizadas en Amazon ECS

Puede crear métricas personalizadas para sus aplicaciones mediante el formato de métricas CloudWatch integrado. El controlador de `awslogs` registro puede interpretar las sentencias de formato métrico CloudWatch incrustadas.

La variable de `CW_CONFIG_CONTENT` entorno del siguiente ejemplo se establece en el contenido del parámetro `cwagentconfig` Systems Manager Parameter Store. Puede ejecutar el agente con esta configuración básica para configurarlo como un punto final con formato métrico integrado. Sin embargo, ya no es necesario.

```
  {
  "logs": {
    "metrics_collected": {
      "emf": { }
    }
  }
}
```

Si tiene implementaciones de Amazon ECS en varias cuentas y regiones, puede usar un AWS Secrets Manager secreto para almacenar su CloudWatch configuración y configurar la política de secretos para compartirla con su organización. Puede utilizar la opción de secretos de la definición de la tarea para establecer la `CW_CONFIG_CONTENT` variable.

Puede usar las bibliotecas de formato métrico integradas de código abierto que se AWS proporcionan en su aplicación y especificar la variable de `AWS_EMF_AGENT_ENDPOINT` entorno para conectarse al contenedor lateral de su CloudWatch agente que actúa como punto final con formato métrico integrado. Por ejemplo, puede utilizar la aplicación Python de ejemplo ecs_cw_emf_example para enviar métricas en formato métrico integrado a CloudWatch un contenedor sidecar de agente configurado como punto final con formato métrico integrado.

El complemento Fluent Bit también se CloudWatch puede utilizar para enviar mensajes en formato métrico incrustado. También puede usar la aplicación Python de ejemplo ecs_firelense_emf_example para enviar métricas en formato métrico integrado a un contenedor sidecar de Firelens for Amazon ECS.

Si no desea utilizar el formato de métricas integrado, puede crear y actualizar las métricas a través de la API o el SDK. CloudWatch AWSAWS No recomendamos este enfoque a menos que tengas un caso de uso específico, ya que añade una sobrecarga de mantenimiento y administración al código.

Registro y monitoreo en Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) se integra con CloudWatch Registros del plano de control de Kubernetes. Amazon EKS proporciona el plano de control como servicio administrado y puedeactivar el registro sin instalar un agente de CloudWatch. La CloudWatch agente también se puede implementar para capturar registros de nodos y contenedores de Amazon EKS. Fluent Bit y Fluentdtambién se admiten para enviar los registros de contenedores a CloudWatch Registros.

CloudWatch Container Insights proporciona una solución completa de monitoreo de métricas para Amazon EKS a nivel de clúster, nodo pod, servicio y servicio. Amazon EKS también admite múltiples opciones para la captura de métricas conPrometheus. El plano de control de Amazon EKSproporciona un punto final de métricasque expone las métricas en un formato Prometheus. Puede implementar Prometheus en su clúster de Amazon EKS para consumir estas métricas.

También puedeConfigurar la CloudWatch Agente para raspar las métricas de Prometheusy crea CloudWatch métricas, además de consumir otros puntos finales de Prometheus. Monitorización de Container Insights para Prometheustambién puede descubrir y capturar automáticamente las métricas de Prometheus a partir de cargas de trabajo y sistemas compatibles y en contenedores.

Puede instalar y configurar la CloudWatch agente en los nodos de Amazon EKS, de forma similar al enfoque utilizado para Amazon EC2 con Distributor y State Manager, para alinear los nodos de Amazon EKS con las configuraciones estándar de registro y supervisión del sistema.

Registro de Amazon EKS

El registro de Kubernetes se puede dividir en registro de planos de control, registro de nodos y registro de aplicaciones. LaPlano de control de Kuberneteses un conjunto de componentes que administran clústeres de Kubernetes y producen registros utilizados para fines de auditoría y diagnóstico. Con Amazon EKS, puedesactivar registros para distintos componentes del plano de controly envíalos a CloudWatch.

Kubernetes también ejecuta componentes del sistema como`kubelet`y`kube-proxy`en cada nodo de Kubernetes que ejecuta tus pods. Estos componentes escriben registros dentro de cada nodo y puede configurar CloudWatch y Container Insights para capturar estos registros para cada nodo de Amazon EKS.

Los contenedores se agrupan comovainasdentro de un clúster de Kubernetes y están programados para ejecutarse en los nodos de Kubernetes. La mayoría de las aplicaciones en contenedores

escriben en salida estándar y error estándar, y el motor de contenedores redirige la salida a un controlador de registro. En Kubernetes, los registros de contenedores se encuentran en el`/var/log/pods`directorio de un nodo. Puede configurar CloudWatch y Container Insights para capturar estos registros para cada uno de los pods de Amazon EKS.

Registro de plano de control de Amazon EKS

Un clúster de Amazon EKS consta de un plano de control de un solo tenant de alta disponibilidad para el clúster de Kubernetes y los nodos de Amazon EKS que ejecutan los contenedores. Los nodos del plano de control se ejecutan en una cuenta administrada porAWS. Los nodos de plano de control de clúster de Amazon EKS están integrados con CloudWatch y puede activar el registro para componentes de planos de control específicos.

Se proporcionan registros para cada instancia de componente del plano de control de Kubernetes.AWSadministra el estado de los nodos del plano de control y proporciona unacuerdo de nivel de servicio (SLA) para el endpoint de Kubernetes.

Registro de nodos y aplicaciones de Amazon EKS

Le recomendamos que utiliceCloudWatch Container Insightspara capturar registros y métricas de Amazon EKS. Container Insights implementa métricas a nivel de clúster, nodo y pod con el CloudWatch agente y Fluent Bit o Fluentd para la captura de registros en CloudWatch. Container Insights también cuenta con paneles automáticos con vistas en capas de su captura CloudWatch Métricas de . Container Insights se implementa como CloudWatch DaemonSet y Fluent Bit DaemonSet que se ejecuta en todos los nodos de Amazon EKS. Container Insights no admite los nodos Fargate porque los nodos son administrados porAWSy no soporta DaemonSets. El registro de Fargate para Amazon EKS se cubre por separado en esta guía.

En la tabla siguiente, se muestra la CloudWatch grupos de registros y registros capturados por elConfiguración predeterminada de captura de registro de Fluentd o Fluent Bitpara Amazon EKS.

`/aws/containerinsights/Cluster_Name/application`	Todos los archivos de registros de`/var/log/containers` . Este directorio proporciona enlaces simbólicos a todos los registros de contenedores de Kubernetes en el`/var/log/pods` Estructura de directori

	os. Esto captura los registros del contenedor de aplicaciones escribiendo `enstdoutostderr`. También incluye registros para contenedores del sistema Kubernetes, tales como`aws-vpc-cni-init`,`kube-proxy` , y`coreDNS`.
`/aws/containerinsights/Cluster_Name/host`	Archivos de registros de`/var/log/dmesg` ,`/var/log/secure` , y`/var/log/messages` .
`/aws/containerinsights/Cluster_Name/dataplane`	Los registros en `/var/log/journal` para `kubelet.service` , `kubeproxy.service` y `docker.service` .

Si no desea utilizar Container Insights con Fluent Bit o Fluentd para registrar, puede capturar registros de nodos y contenedores con el CloudWatch Agente instalado en nodos de Amazon EKS. Los nodos de Amazon EKS son instancias EC2, lo que significa que debe incluirlos en el enfoque de registro estándar a nivel de sistema para Amazon EC2. Si instala el CloudWatch agente mediante Distributor y State Manager, luego los nodos de Amazon EKS también se incluyen en el CloudWatch instalación, configuración y actualización del agente.

En la tabla siguiente se muestran los registros específicos de Kubernetes y que debe capturar si no utiliza Container Insights con Fluent Bit o Fluentd para registrar.

`/var/log/containers`	Este directorio proporciona enlaces simbólicos a todos los registros de contenedores de Kubernetes en el`/var/log/pods` Estructura de directorios. Esto captura eficazmente los registros del contenedor de aplicaciones escribiendo `enstdoutostderr`. Esto incluye registros de contenedores del sistema de Kubernetes, tales como`aws-vpc-cni-init`,`kube-proxy` , y`coreDNS`. Importante: Esto no es obligatorio si utiliza Container Insights.

`var/log/aws-routed-eni/ipamd.log`
 	
`/var/log/aws-routed-eni/plugin.log`
	Los registros del daemon L-IPAM se pueden encontrar aquí

Debe asegurarse de que los nodos de Amazon EKS instalen y configuren el CloudWatch agente para enviar registros y métricas de nivel de sistema adecuados. Sin embargo, la AMI optimizada de Amazon EKS no incluye el agente de Systems Manager. Usandoplantillas de lanzamiento, puede automatizar la instalación del agente de Systems Manager y un valor predeterminado CloudWatch configuración que captura registros específicos importantes de Amazon EKS con un script de inicio implementado a través de la sección de datos de usuario. Los nodos de Amazon EKS se implementan mediante un grupo de Auto Scaling comogrupo de nodos administradoso comonodos autoadministrados.

Con los grupos de nodos administrados, suministra unplantilla de lanzamientoque incluye la sección de datos de usuario para automatizar la instalación del agente de Systems Manager y CloudWatch Configuración de . Puede personalizar y utilizar elamazon_eks_managed_node_group_launch_config.yaml AWS CloudFormationplantilla para crear una plantilla de lanzamiento que instale el agente de Systems Manager, CloudWatch agente, y también añade una configuración de registro específica de Amazon EKS a la CloudWatch directorio de configuración. Esta plantilla se puede utilizar para actualizar la plantilla de lanzamiento de grupos de nodos administrados de Amazon EKS con un infrastructure-as-code (iAC). Cada actualización de laAWS CloudFormationLa plantilla aprovisiona una nueva versión de la plantilla de lanzamiento. A continuación, puede actualizar el grupo de nodos para utilizar la nueva versión de plantilla y tener laproceso de ciclo de vida administradoactualiza tus nodos sin tiempo de inactividad. Asegúrese de que el perfil de instancia e rol de IAM aplicado a su grupo de nodos administrado incluya el`CloudWatchAgentServerPolicy`y`AmazonSSMManagedInstanceCore` AWSpolíticas administradas.

Con los nodos autoadministrados, aprovisiona y administra directamente el ciclo de vida y la estrategia de actualización de los nodos de Amazon EKS. Los nodos autoadministrados le permiten ejecutar nodos de Windows en su clúster de Amazon EKS yBottlerocket, junto conotras opciones. Puede utilizarAWS CloudFormationpara implementar nodos autogestionados en los clústeres de Amazon EKS, lo que significa que puede utilizar un enfoque de cambio administrado y iAC para los clústeres de Amazon EKS.AWSproporciona laamazon-eks-nodegroup.yaml AWS CloudFormationplantilla que puede usar tal cual o personalizar. La plantilla aprovisiona todos los

recursos necesarios para los nodos de Amazon EKS de un clúster (por ejemplo, un rol de IAM independiente, un grupo de seguridad, un grupo de Amazon EC2 Auto Scaling y una plantilla de lanzamiento). Laamazon-eks-nodegroup.yaml AWS CloudFormationplantilla es una versión actualizada que instala el agente de Systems Manager requerido, CloudWatch agente, y también añade una configuración de registro específica de Amazon EKS a la CloudWatch directorio de configuración.

Registro para Amazon EKS en Fargate

Con Amazon EKS en Fargate, puedes implementar pods sin asignar ni administrar tus nodos de Kubernetes. Esto elimina la necesidad de capturar registros de nivel de sistema para los nodos de Kubernetes. Para capturar los registros de los pods de Fargate, puedes usar Fluent Bit para reenviar los registros directamente a CloudWatch. Esto le permite enrutar automáticamente los registros a CloudWatch sin más configuración ni contenedor sidecar para tus pods de Amazon EKS en Fargate. Para obtener más información sobre este tema, consulteRegistros de Fargateen la documentación de Amazon EKS yBroca fluida para Amazon EKSen elAWSBlog. Esta solución captura el`STDOUT`y`STDERR`las secuencias de entrada/salida (E/S) del contenedor y las envía a CloudWatch a través de Fluent Bit, basada en la configuración de bits fluentes establecida para el clúster de Amazon EKS en Fargate.

Métricas de Amazon EKS y Kubernetes

Kubernetes proporciona una API de métricas que le permite acceder a las métricas de uso de recursos (por ejemplo, uso de CPU y memoria para nodos y pods), pero la API solo proporciona información puntual y no métricas históricas. LaServidor de métricas de Kubernetesse utiliza normalmente para implementaciones de Amazon EKS y Kubernetes para agregar métricas, proporcionar información histórica a corto plazo sobre métricas y funciones de soporte tales comoEscalador automático de pods horizontales.

Amazon EKS expone las métricas del plano de control a través del servidor API de Kubernetesen formato Prometheusy CloudWatch puede capturar e ingerir estas métricas. CloudWatch y Container Insights también se puede configurar para proporcionar captura, análisis y alarma de métricas completas para sus nodos y pods de Amazon EKS.

Métricas del plano de control de Kubernetes

Kubernetes expone las métricas del plano de control en formato Prometheus mediante el`/metrics`Endpoint API HTTP. Deberías instalarPrometheusen el clúster de Kubernetes para graficar

y ver estas métricas con un navegador web. También puedeingerir las métricas expuestaspor el servidor API de Kubernetes en CloudWatch.

Métricas de nodos y sistemas para Kubernetes

Kubernetes proporciona el PrometheusServidor de métricascápsula que puedesdesplegar y ejecutaren los clústeres de Kubernetes para estadísticas de memoria y CPU a nivel de clúster, nodo y pod. Estas métricas se utilizan con elEscalador automático de pods horizontalesyEscalador automático vertical de pods. CloudWatch también puede proporcionar estas métricas.

Debe instalar Kubernetes Metrics Server si utiliza elPanel de Kubernetesо los escaladores automáticos de pods horizontales y verticales. El panel de Kubernetes le ayuda a explorar y configurar el clúster, los nodos, los pods y la configuración relacionada de Kubernetes, y ver las métricas de CPU y memoria desde el servidor de métricas de Kubernetes. Puede implementar esta solución para clústeres individuales siguiendo los pasos delImplementar el panel de Kubernetesen la documentación de Amazon EKS.

Las métricas proporcionadas por Kubernetes Metrics Server no se pueden utilizar para fines de escalado no automático (por ejemplo, supervisión). Las métricas están pensadas para point-in-time análisis y no análisis histórico. El panel de Kubernetes implementa el`dashboard-metrics-scraper`para almacenar métricas desde el servidor de métricas de Kubernetes durante un breve período de tiempo.

Container Insights utiliza una versión contenerizada del CloudWatch agente que se ejecuta en un Kubernetes DaemonSet para descubrir todos los contenedores en ejecución de un clúster y proporcionar métricas a nivel de nodos. Recopila datos de rendimiento en cada nivel de la pila de rendimiento. Puede utilizar el inicio rápido de desdeAWSInicio rápido o configure Container Insights por separado. El inicio rápido configura la supervisión de métricas con la CloudWatch agente y registro con Fluent Bit, por lo que solo necesita implementarlo una vez para registrar y supervisar.

Dado que los nodos de Amazon EKS son instancias EC2, debe capturar métricas a nivel de sistemas, además de las métricas capturadas por Container Insights, utilizando los estándares definidos para Amazon EC2. Puede utilizar el mismo enfoque desde laConfigurar State Manager y distribuidor para CloudWatch implementación y configuración de agentesde esta guía para instalar y configurar la CloudWatch Agente de los clústeres de Amazon EKS. Puede actualizar el archivo de configuración de CloudWatch específico de Amazon EKS para incluir métricas y configuración de registro específica de Amazon EKS.

La CloudWatch agente con soporte de Prometheus puede descubrir y eliminar automáticamente las métricas de Prometheus decargas de trabajo y sistemas compatibles y en contenedores. Los ingiere como CloudWatch registros en formato métrico incrustado para análisis con CloudWatch Registra Insights y crea automáticamente métricas de CloudWatch.

> **Important**
>
> Debeimplementar una versión especializadadel CloudWatch para recopilar métricas de Prometheus. Se trata de un agente independiente del CloudWatch Agente implementado para Container Insights. Puede utilizar elprometheus_jmxaplicación Java de ejemplo, que incluye los archivos de implementación y configuración para el CloudWatch implementación de pods de agente y Amazon EKS para demostrar el descubrimiento de métricas de Prometheus. Para obtener más información, consulteConfigure la carga de trabajo de muestra de Java/JMX en Amazon EKS y Kubernetesen la documentación de CloudWatch. También puede configurar la CloudWatch agente para capturar métricas de otros destinos de Prometheus que se ejecutan en su clúster de Amazon EKS.

Métricas de aplicación

Puede crear sus propias métricas personalizadas con laFormato de métricas integradas de CloudWatch. Para ingerir sentencias de formato métrico incrustadas, debe enviar entradas de formato métrico incrustado a un extremo de formato métrico incrustado. La CloudWatch agente se puede configurar comocontenedor sidecar en tu pod Amazon EKS. La CloudWatch la configuración del agente se almacena como Kubernetes ConfigMap y lee por tu CloudWatch agent sidecar container para iniciar el extremo de formato métrico incrustado.

También puede configurar su aplicación como objetivo de Prometheus y configurar el agente de CloudWatch, con soporte de Prometheus, para descubrir, extraer e incorporar sus métricas en CloudWatch. Por ejemplo, puede utilizar laexportador JMX de código abiertocon sus aplicaciones Java para exponer JMX Beans para el consumo de Prometheus por el CloudWatch agente.

Si no desea utilizar el formato de métrica incrustado, también puede crear y actualizar métricas de CloudWatch mediante AWSAPIoAWS SDK. Sin embargo, no recomendamos este enfoque porque mezcla el monitoreo y la lógica de la aplicación.

Métricas de Amazon EKS en Fargate

Fargate aprovisiona automáticamente los nodos de Amazon EKS para ejecutar los pods de Kubernetes para que no tengas que supervisar ni recopilar métricas a nivel de nodos. Sin embargo, debes supervisar las métricas de los pods que se ejecutan en tus nodos de Amazon EKS en Fargate. Container Insights no está disponible actualmente para Amazon EKS en Fargate porque requiere las siguientes capacidades que no son compatibles actualmente:

- Actualmente no se admiten DaemonSets. Container Insights se implementa ejecutando el CloudWatch Agente como DaemonSet en cada nodo de clúster.
- No se admiten los volúmenes persistentes HostPath. La CloudWatch agent container utiliza volúmenes persistentes HostPath como requisito previo para recopilar datos de métricas de contenedor.
- Fargate impide los contenedores privilegiados y el acceso a la información del host.

Puede utilizar elenrutador de registro incorporado para Fargatepara enviar declaraciones de formato de métricas integradas a CloudWatch. El enrutador de registros utiliza Fluent Bit, que tiene CloudWatch complemento que se puede configurar para admitir sentencias de formato métrico incrustadas.

Puede recuperar y capturar métricas a nivel de pod para sus nodos Fargate implementando el servidor Prometheus en su clúster de Amazon EKS para recopilar métricas de los nodos de Fargate. Dado que Prometheus requiere almacenamiento persistente, puede implementar Prometheus en Fargate si utiliza Amazon Elastic File System (Amazon EFS) para almacenamiento persistente. También puede implementar Prometheus en un nodo respaldado de Amazon EC2. Para obtener más información, consulteSupervisar Amazon EKS enAWS Fargateusando Prometheus y Grafanaen elAWSBlog.

Supervisión de Prometheus en Amazon EKS

Amazon Managed Service for Prometheusproporciona un sistema escalable, seguro,AWSservicio administrado para Prometheus de código abierto. Puede utilizar el lenguaje de consultas de Prometheus (ProMQL) para supervisar el rendimiento de las cargas de trabajo en contenedores sin administrar la infraestructura subyacente para ingerir, almacenar y consultar métricas operativas. Puede recopilar métricas de Prometheus de Amazon EKS y Amazon ECS utilizandoAWSDistro for OpenTelemetry (ADOT)o servidores Prometheus como agentes de recopilación.

Supervisión de CloudWatch Container Insights para Prometheusle permite configurar y utilizar el CloudWatch agente para descubrir las métricas de Prometheus de las cargas de trabajo de Amazon ECS, Amazon EKS y Kubernetes, e incorporarlas como métricas de CloudWatch. Esta solución es apropiada si CloudWatch es su principal solución de observabilidad y monitoreo. Sin embargo, en la siguiente lista se describen los casos de uso en los que Amazon Managed Service for Prometheus proporciona más flexibilidad para ingerir, almacenar y consultar métricas de Prometheus:

- Amazon Managed Service for Prometheus le permite utilizar los servidores Prometheus existentes implementados en Amazon EKS o Kubernetes autoadministrados y configurarlos para que escriban en Amazon Managed Service for Prometheus en lugar de un data store configurado localmente. Esto elimina la pesada carga indiferenciada de administrar un data store de alta disponibilidad para sus servidores Prometheus y su infraestructura. Amazon Managed Service for Prometheus es una opción adecuada cuando tiene una implementación de Prometheus madura que desea aprovechar en elAWSCloud Cloud.
- Grafana admite directamente a Prometheus como fuente de datos para visualización. Si desea utilizar Grafana con Prometheus en lugar de CloudWatch Los paneles de control para la supervisión de contenedores y Amazon Managed Service for Prometheus podrían cumplir sus requisitos. Amazon Managed Service for Prometheus se integra con Amazon Managed Grafana para proporcionar una solución administrada de monitoreo y visualización de código abierto.
- Prometheus le permite realizar análisis de sus métricas operativas mediante consultas ProMQL. En cambio,la CloudWatch agente ingiere métricas de Prometheus en formato de métricas integradasen CloudWatch Registros que dan como resultado CloudWatch Métricas de . Puede consultar los registros de formato de métricas integradas mediante CloudWatch Logs Insights.
- Si no planea utilizar CloudWatch para monitorear y capturar métricas, debe utilizar Amazon Managed Service for Prometheus con su servidor Prometheus y una solución de visualización como Grafana. Necesitas configurar tu servidor Prometheus para extraer métricas de tus destinos de Prometheus y configurar el servidor paraescritura remota en su espacio de trabajo de

Amazon Managed Service for Prometheus. Si utilizas Amazon Managed Grafana, puedesintegre directamente Amazon Managed Grafana con su fuente de datos de Amazon Managed Service for Prometheus mediante el complemento incluido. Dado que los datos de métricas se almacenan en Amazon Managed Service for Prometheus, no existe ninguna dependencia para implementar el CloudWatch agente o requisito de ingerir datos en CloudWatch. La CloudWatch es obligatorio para la supervisión de Container Insights de Prometheus.

También puede utilizar ADOT Collector para extraer de una aplicación instrumentada por Prometheus y enviar las métricas a Amazon Managed Service for Prometheus. Para obtener más información sobre ADOT Collector, consulte laAWSDistro for OpenTelemetry.

Registro y métricas paraAWS Lambda

Lambdaelimina la necesidad de gestionar y supervisar los servidores para sus cargas de trabajo y funciona automáticamente con CloudWatchMétricas y CloudWatch Registra sin necesidad de configurar o instrumentar el código de la aplicación. Esta sección le ayuda a comprender las características de rendimiento de los sistemas utilizados por Lambda y cómo sus elecciones de configuración influyen en el rendimiento. También le ayuda a registrar y supervisar las funciones de Lambda para optimizar el rendimiento y diagnosticar problemas a nivel de aplicación.

Registro de funciones lambda

Lambda transmite automáticamente la salida estándar y los mensajes de error estándar de una función de Lambda a CloudWatch Registra, sin necesidad de registrar controladores. Lambda también aprovisiona automáticamente los contenedores en los que se ejecuta la función de Lambda y los configura para que generen los mensajes de registro en flujos de registro independientes.

Las invocaciones posteriores de la función de Lambda pueden reutilizar el mismo contenedor y generar resultados en el mismo flujo de registro. Lambda también puede aprovisionar un nuevo contenedor y enviar la invocación a un nuevo flujo de registro.

Lambda crea automáticamente un grupo de registros cuando se invoca la función de Lambda por primera vez. Las funciones de Lambda pueden tener varias versiones y usted puede elegir la versión que desee ejecutar. Todos los registros de las invocaciones de la función de Lambda se almacenan en el mismo grupo de registros. El nombre no se puede cambiar y está en el`/aws/lambda/<YourLambdaFunctionName>`formato. Se crea un flujo de registro independiente en el grupo de registros para cada instancia de función de Lambda. Lambda tiene una convención de nomenclatura estándar para los flujos de registro que utiliza un`YYYY/MM/DD/[<FunctionVersion>]<InstanceId>`formato. El`InstanceId`es generado porAWSpara identificar la instancia de la función Lambda.

Le recomendamos que formatee los mensajes de registro en formato JSON, ya que puede consultarlos más fácilmente con CloudWatch Registra Insights. También se pueden filtrar y exportar más fácilmente. Puede usar una biblioteca de registro para simplificar este proceso o escribir sus propias funciones de manejo de registros. Le recomendamos que utilice una biblioteca de registro para ayudar a formatear y clasificar los mensajes de registro. Por ejemplo, si la función Lambda está escrita en Python, puede usar laMódulo de registro de Pythonpara registrar los mensajes y

controlar el formato de salida. Lambda utiliza de forma nativa la biblioteca de registro de Python para las funciones de Lambda escritas en Python, y usted puede recuperar y personalizar el registrador dentro de su función de Lambda.AWS Labs ha creado elAWSLambda Powertools para Pythonkit de herramientas para desarrolladores que facilita el enriquecimiento de los mensajes de registro con datos clave, como los arranques en frío. El kit de herramientas está disponible para Python, Java, TypeScript y.NET.

Otra práctica recomendada es establecer el nivel de salida del registro mediante una variable y ajustarlo en función del entorno y sus requisitos. El código de la función Lambda, además de las bibliotecas utilizadas, podría generar una gran cantidad de datos de registro en función del nivel de salida del registro. Esto puede afectar a los costes de registro y al rendimiento.

Lambda le permite configurar variables de entorno para su entorno de ejecución de funciones de Lambda sin necesidad de actualizar el código. Por ejemplo, puede crear un`LAMBDA_LOG_LEVEL`variable de entorno que define el nivel de salida del registro que puede recuperar del código. En el siguiente ejemplo se intenta recuperar un`LAMBDA_LOG_LEVEL`variable de entorno y utilice el valor para definir el resultado del registro. Si la variable de entorno no está establecida, el valor predeterminado es`INFO`nivel.

```
import logging
from os import getenv

logger = logging.getLogger()
log_level = getenv("LAMBDA_LOG_LEVEL", "INFO")
level = logging.getLevelName(log_level)
logger.setLevel(level)
```

Envío de registros a otros destinos desde CloudWatch

Puede enviar registros a otros destinos (por ejemplo, Amazon OpenSearch Servicio (o una función de Lambda) mediante filtros de suscripción. Si no utilizas Amazon OpenSearch Servicio, puede utilizar una función de Lambda para procesar los registros y enviarlos a unAWSservicio de su elección mediante elAWSSDK.

También puede utilizar los SDK para destinos de registro ajenos alAWSIntegre su función de Lambda para enviar directamente las declaraciones de registro al destino que elija. Si elige esta

opción, le recomendamos que considere el impacto de la latencia, el tiempo de procesamiento adicional, la gestión de errores y reintentos y la vinculación de la lógica operativa a la función de Lambda.

Métricas de función de Lambda

Lambda le permite ejecutar su código sin administrar ni escalar los servidores, lo que prácticamente elimina la carga de realizar auditorías y diagnósticos a nivel del sistema. Sin embargo, sigue siendo importante comprender las métricas de rendimiento e invocación a nivel del sistema para las funciones de Lambda. Esto le ayuda a optimizar la configuración de los recursos y a mejorar el rendimiento del código. La supervisión y la medición eficaces del rendimiento pueden mejorar la experiencia del usuario y reducir los costes al dimensionar adecuadamente las funciones de Lambda. Por lo general, las cargas de trabajo que se ejecutan como funciones de Lambda también tienen métricas a nivel de aplicación que deben capturarse y analizarse. Lambda admite directamente el formato métrico integrado para que la captura se realice a nivel de aplicación CloudWatch las métricas son más fáciles.

Métricas a nivel de sistema

Lambda se integra automáticamente con CloudWatch Métrica y proporciona un conjunto demétricas estándar para sus funciones de Lambda. Lambda también proporciona un panel de supervisión independiente para cada función de Lambda con estas métricas. Dos métricas importantes que debe supervisar son los errores y los errores de invocación. Comprender las diferencias entre los errores de invocación y otros tipos de errores le ayuda a diagnosticar y respaldar las implementaciones de Lambda.

Errores de invocaciónimpiden que la función Lambda se ejecute. Estos errores se producen antes de que se ejecute el código, por lo que no puede implementar la gestión de errores en el código para identificarlos. En su lugar, debe configurar alarmas para las funciones de Lambda que detecten estos errores y notifiquen a los propietarios de las operaciones y la carga de trabajo. Estos errores suelen estar relacionados con un error de configuración o permiso y pueden producirse debido a un cambio en la configuración o los permisos. Los errores de invocación pueden iniciar un reintento, lo que provoca varias invocaciones de la función.

Una función de Lambda que se invoca correctamente devuelve una respuesta HTTP 200 incluso si la función lanza una excepción. Sus funciones de Lambda deben implementar la gestión de errores y generar excepciones para que`Errors`la métrica captura e identifica las ejecuciones fallidas de la

función de Lambda. Debe devolver una respuesta formateada a las invocaciones de la función de Lambda que incluya información para determinar si la ejecución ha fallado total, parcialmente o se ha realizado correctamente.

CloudWatch proveeCloudWatch Lambda Insightsque puede habilitar para una función Lambda individual. Lambda Insights recopila, agrega y resume las métricas a nivel del sistema (por ejemplo, el tiempo de CPU, la memoria, el disco y el uso de la red). Lambda Insights también recopila, agrega y resume la información de diagnóstico (por ejemplo, arranques en frío y paradas de trabajo de Lambda) para ayudarlo a aislar los problemas y resolverlos rápidamente.

Lambda Insights utiliza el formato métrico integrado para emitir automáticamente la información de rendimiento al`/aws/lambda-insights/`grupo de registros con un prefijo de nombre de flujo de registro basado en el nombre de la función de Lambda. Estos eventos del registro de rendimiento crean CloudWatch métricas que son la base de la automatización CloudWatch cuadros de mando. Le recomendamos que habilite Lambda Insights para las pruebas de rendimiento y los entornos de producción. Entre las métricas adicionales creadas por Lambda Insights se incluyen`memory_utilization`esto ayuda a dimensionar correctamente las funciones de Lambda para evitar tener que pagar por una capacidad innecesaria.

Métricas de aplicación

También puede crear y capturar las métricas de sus propias aplicaciones en CloudWatch utilizando el formato métrico integrado. Puede aprovecharAWS proporcionó bibliotecas para el formato métrico integradopara crear y emitir declaraciones de formato métrico integradas a CloudWatch. La Lambda integrada CloudWatch La función de registro está configurada para procesar y extraer sentencias de formato métrico integradas con el formato adecuado.

Búsqueda y análisis de registros CloudWatch

Una vez capturados los registros y las métricas en un formato y una ubicación coherentes, puede buscarlos y analizarlos para ayudar a mejorar la eficiencia operativa, además de identificar los problemas y solucionarlos. Le recomendamos que capture los registros en un formato correcto (por ejemplo, JSON) para facilitar la búsqueda y el análisis de los registros. La mayoría de las cargas de trabajo utilizan una colección deAWS recursos como redes, procesamiento, almacenamiento y bases de datos. Siempre que sea posible, debe analizar colectivamente las métricas y los registros de estos recursos y correlacionarlos para supervisar y gestionar de manera eficaz todas susAWS cargas de trabajo.

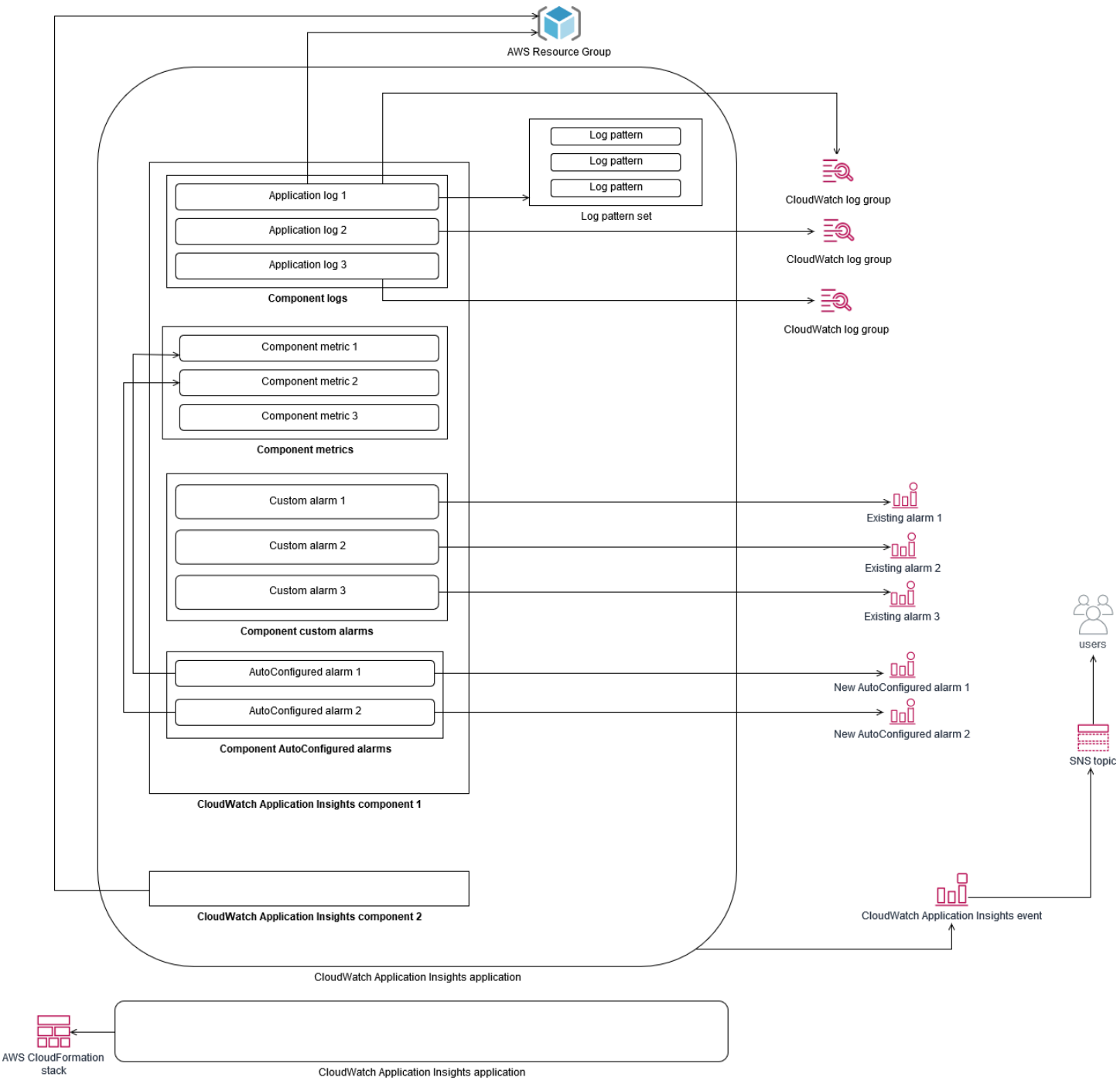
CloudWatch proporciona varias funciones para ayudar a analizar los registros y las métricas, como CloudWatch Application Insights para definir y monitorear colectivamente las métricas y los registros de una aplicación en diferentesAWS recursos,CloudWatch la detección de anomalías para detectar anomalías para su métricas e información deCloudWatch registro para buscar y analizar de forma interactiva los datos de registro CloudWatch en.

Supervise y analice las aplicaciones de forma colectiva con CloudWatch Application Insights

Los propietarios de aplicaciones pueden usar Amazon CloudWatch Application Insights para configurar la supervisión y el análisis automáticos de las cargas de trabajo. Esto se puede configurar además del monitoreo estándar a nivel de sistemas configurado para todas las cargas de trabajo de una cuenta. Configurar el monitoreo a través de CloudWatch Application Insights también puede ayudar a los equipos de aplicaciones a alinearse de manera proactiva con las operaciones y reducir el tiempo medio de recuperación (MTTR). CloudWatch Application Insights puede ayudar a reducir el esfuerzo necesario para establecer el registro y la supervisión a nivel de la aplicación. También proporciona un marco basado en componentes que ayuda a los equipos a dividir las responsabilidades de registro y monitoreo.

CloudWatch Application Insights utiliza grupos de recursos para identificar los recursos que deben supervisarse colectivamente como una aplicación. Los recursos compatibles del grupo de recursos se convierten en componentes definidos individualmente de su CloudWatch aplicación Application Insights. Cada componente de la CloudWatch aplicación Application Insights tiene sus propios registros, métricas y alarmas.

Para los registros, usted define el conjunto de patrones de registro que debe usarse para el componente y dentro de su CloudWatch aplicación Application Insights. Un conjunto de patrones de registro es un conjunto de patrones de registro que se buscan en función de expresiones regulares, junto con una gravedad baja, media o alta cuando se detecta el patrón. En el caso de las métricas, elige las métricas que desea supervisar para cada componente de una lista de métricas compatibles y específicas del servicio. Para las alarmas, CloudWatch Application Insights crea y configura automáticamente alarmas estándar o de detección de anomalías para las métricas que se supervisan. CloudWatch Application Insights tiene configuraciones automáticas para las métricas y la captura de registros para las tecnologías descritas en los registros y las métricas compatibles con CloudWatch Application Insights en la CloudWatch documentación. El siguiente diagrama muestra las relaciones entre los componentes de CloudWatch Application Insights y sus configuraciones de registro y monitoreo. Cada componente ha definido sus propios registros y métricas para monitorizarlos mediante CloudWatch registros y métricas.



Las instancias de EC2 supervisadas por CloudWatch Application Insights requieren un Systems Manager, CloudWatch agentes y permisos. Para obtener más información al respecto, consulte Requisitos previos para configurar una CloudWatch aplicación con Application Insights en la CloudWatch documentación. CloudWatch Application Insights utiliza Systems Manager para instalar y actualizar el CloudWatch agente. Las métricas y los registros configurados en CloudWatch Application Insights crean un archivo de configuración del CloudWatch agente que se almacena

en un parámetro de Systems Manager con el`AmazonCloudWatch-ApplicationInsights-SSMParameter` prefijo de cada componente de CloudWatch Application Insights. Esto da como resultado que se agregue un archivo de configuración de agentes independiente CloudWatch al directorio de configuración del CloudWatch agente de la instancia EC2. Se ejecuta un comando de Systems Manager para añadir esta configuración a la configuración activa de la instancia EC2. El uso CloudWatch de Application Insights no afecta a los ajustes de configuración de los CloudWatch agentes existentes. Puede usar CloudWatch Application Insights además de sus propias configuraciones de CloudWatch agentes a nivel de sistema y aplicación. Sin embargo, debe asegurarse de que las configuraciones no se superpongan.

Realizar análisis de CloudWatch registros con Logs Insights

CloudWatch Logs Insights facilita la búsqueda en varios grupos de registros mediante un lenguaje de consulta sencillo. Si los registros de su aplicación están estructurados en formato JSON, CloudWatch Logs Insights descubre automáticamente los campos JSON en sus flujos de registro en varios grupos de registros. Puede usar CloudWatch Logs Insights para analizar los registros de su aplicación y sistema, lo que guarda sus consultas para usarlas en el future. La sintaxis de consulta de CloudWatch Logs Insights admite funciones como la agregación con funciones, por ejemplo, sum (), avg (), count (), min () y max (), que pueden resultar útiles para solucionar problemas de las aplicaciones o analizar el rendimiento.

Si utiliza el formato de métrica incrustada para crear CloudWatch métricas, puede consultar sus registros de formato métrico incrustado para generar métricas únicas mediante las funciones de agregación compatibles. Esto ayuda a reducir los costos de CloudWatch monitoreo al capturar los puntos de datos necesarios para generar métricas específicas según sea necesario, en lugar de capturarlos activamente como métricas personalizadas. Esto es especialmente eficaz para dimensiones con una cardinalidad alta que darían como resultado una gran cantidad de métricas. CloudWatch Container Insights también adopta este enfoque y captura datos de rendimiento detallados, pero solo genera CloudWatch métricas para un subconjunto de estos datos.

Por ejemplo, la siguiente entrada métrica incrustada solo genera un conjunto limitado de CloudWatch métricas a partir de los datos métricos capturados en la declaración de formato métrico incrustado:

```
{
 "AutoScalingGroupName": "eks-e0bab7f4-fa6c-64ba-dbd9-094aee6cf9ba",
 "CloudWatchMetrics": [
 {
 "Metrics": [
```

```
{
"Unit": "Count",
"Name": "pod_number_of_container_restarts"
}
],
"Dimensions": [
[
"PodName",
"Namespace",
"ClusterName"
]
],
"Namespace": "ContainerInsights"
}
],
"ClusterName": "eksdemo",
"InstanceId": "i-03b21a16b854aa4ca",
"InstanceType": "t3.medium",
"Namespace": "amazon-cloudwatch",
"NodeName": "ip-172-31-10-211.ec2.internal",
"PodName": "cloudwatch-agent",
"Sources": [
"cadvisor",
"pod",
"calculated"
],
"Timestamp": "1605111338968",
"Type": "Pod",
"Version": "0",
"pod_cpu_limit": 200,
"pod_cpu_request": 200,
"pod_cpu_reserved_capacity": 10,
"pod_cpu_usage_system": 3.268605094109382,
"pod_cpu_usage_total": 8.899539221131045,
"pod_cpu_usage_user": 4.160042847048305,
"pod_cpu_utilization": 0.44497696105655227,
"pod_cpu_utilization_over_pod_limit": 4.4497696105655224,
"pod_memory_cache": 4096,
"pod_memory_failcnt": 0,
"pod_memory_hierarchical_pgfault": 0,
"pod_memory_hierarchical_pgmajfault": 0,
"pod_memory_limit": 209715200,
"pod_memory_mapped_file": 0,
```

```
 "pod_memory_max_usage": 43024384,
 "pod_memory_pgfault": 0,
 "pod_memory_pgmajfault": 0,
 "pod_memory_request": 209715200,
 "pod_memory_reserved_capacity": 5.148439982463127,
 "pod_memory_rss": 38481920,
 "pod_memory_swap": 0,
 "pod_memory_usage": 42803200,
 "pod_memory_utilization": 0.6172094650851303,
 "pod_memory_utilization_over_pod_limit": 11.98828125,
 "pod_memory_working_set": 25141248,
 "pod_network_rx_bytes": 3566.4174629544723,
 "pod_network_rx_dropped": 0,
 "pod_network_rx_errors": 0,
 "pod_network_rx_packets": 3.3495665260575094,
 "pod_network_total_bytes": 4283.442421354973,
 "pod_network_tx_bytes": 717.0249584005006,
 "pod_network_tx_dropped": 0,
 "pod_network_tx_errors": 0,
 "pod_network_tx_packets": 2.6964010534762948,
 "pod_number_of_container_restarts": 0,
 "pod_number_of_containers": 1,
 "pod_number_of_running_containers": 1,
 "pod_status": "Running"
}
```


Sin embargo, puede consultar las métricas capturadas para obtener más información. Por ejemplo, puede ejecutar la siguiente consulta para ver los 20 módulos más recientes con errores de página de memoria:

```
fields @timestamp, @message
| filter (pod_memory_pgfault > 0)
| sort @timestamp desc
| limit 20
```

Realizar análisis de registros con Amazon OpenSearch Service

CloudWatch se integra con Amazon OpenSearch Service al permitirle transmitir los datos de CloudWatch registro de los grupos de registros a un clúster de Amazon OpenSearch Service de su elección con un filtro de suscripción. Puedes usarlo CloudWatch para la captura y el análisis de

registros y métricas principales y, a continuación, aumentarlos con Amazon OpenSearch Service para los siguientes casos de uso:

- Control detallado del acceso a los datos: Amazon OpenSearch Service te permite limitar el acceso a los datos a nivel de campo y ayuda a anonimizar los datos de los campos según los permisos de los usuarios. Esto es útil si desea soporte para la solución de problemas sin exponer datos confidenciales.
- Agrega y busca registros en varias cuentas, regiones e infraestructuras: puedes transmitir tus registros de varias cuentas y regiones a un clúster de Amazon OpenSearch Service común. Sus equipos de operaciones centralizadas pueden analizar tendencias y problemas y realizar análisis en todas las cuentas y regiones. La transmisión de CloudWatch registros a Amazon OpenSearch Service también te ayuda a buscar y analizar una aplicación multirregional en una ubicación central.
- Envíe y enriquezca los registros directamente a Amazon OpenSearch Service mediante ElasticSearch agentes: los componentes de su pila de aplicaciones y tecnologías pueden utilizar sistemas operativos que no sean compatibles con el CloudWatch agente. También puede que desee enriquecer y transformar los datos de registro antes de enviarlos a su solución de registro. Amazon OpenSearch Service admite clientes de Elasticsearch estándar, como los remitentes de datos de la familia Elastic Beats y Logstash, que permiten el enriquecimiento y la transformación de los registros antes de enviar los datos de registro a Amazon OpenSearch Service.
- La solución de administración de operaciones existente utiliza unaElasticSearch pila Logstash y Kibana (ELK) para el registro y la supervisión. Es posible que ya tenga una inversión significativa en Amazon OpenSearch Service o Elasticsearch de código abierto con muchas cargas de trabajo ya configuradas. Es posible que también tengas paneles operativos que se hayan creado en Kibana y quieras seguir usando.

Si no piensas usar CloudWatch registros, puedes usar agentes, controladores de registros y bibliotecas compatibles con Amazon OpenSearch Service (por ejemplo, Fluent Bit, Fluentd, logstash y Open Distro for ElasticSearch API) para enviar tus registros directamente a Amazon OpenSearch Service y omitirlos CloudWatch. Sin embargo, también debe implementar una solución para capturar los registros generados porAWS los servicios. CloudWatch Los registros son la principal solución de captura de registros para muchosAWS servicios y varios servicios crean automáticamente nuevos grupos de registros en CloudWatch. Por ejemplo, Lambda crea un nuevo grupo de registros para cada función de Lambda. Puedes configurar un filtro de suscripción para que un grupo de registros transmita sus registros a Amazon OpenSearch Service. Puede configurar

manualmente un filtro de suscripción para cada grupo de registro individual que desee transmitir a Amazon OpenSearch Service. Como alternativa, puede implementar una solución que suscriba automáticamente nuevos grupos de registros a los ElasticSearch clústeres. Puede transmitir los registros a un ElasticSearch clúster en la misma cuenta o a una cuenta centralizada. La transmisión de registros a un ElasticSearch clúster en la misma cuenta ayuda a los propietarios de las cargas de trabajo a analizar y soportar mejor sus cargas de trabajo.

Debería considerar la posibilidad de configurar un ElasticSearch clúster en una cuenta centralizada o compartida para agregar registros en sus cuentas, regiones y aplicaciones. Por ejemplo,AWS Control Tower configura una cuenta de Log Archive que se utiliza para el registro centralizado. Cuando se crea una nueva cuenta enAWS Control Tower, susAWS CloudTrailAWS Config registros se envían a un bucket de S3 en esta cuenta centralizada. El registro instrumentado porAWS Control Tower es para el registro de configuraciones, cambios y auditorías.

Para establecer una solución centralizada de análisis de registros de aplicaciones con Amazon OpenSearch Service, puede implementar uno o más clústeres de Amazon OpenSearch Service centralizados en su cuenta de registro centralizada y configurar grupos de registros en sus otras cuentas para transmitir los registros al Amazon OpenSearch Service centralizado. clústeres.

Puede crear clústeres OpenSearch de Amazon Service independientes para gestionar diferentes aplicaciones o capas de su arquitectura de nube que podrían distribuirse en sus cuentas. El uso de clústeres de Amazon OpenSearch Service independientes le ayuda a reducir los riesgos de seguridad y disponibilidad, y tener un clúster de Amazon OpenSearch Service común puede facilitar la búsqueda y la relación de datos dentro del mismo clúster.

Opciones alarmantes con CloudWatch

Realizar un análisis automatizado y único de métricas importantes le ayuda a detectar y resolver problemas antes de que afecten a sus cargas de trabajo. CloudWatch facilita el gráfico y la comparación de varias métricas mediante el uso de varias estadísticas durante un período de tiempo específico. Puede usar CloudWatch para buscar en todas las métricas con los valores de dimensión necesarios para encontrar las métricas que necesita para el análisis.

Le recomendamos que comience su enfoque de captura de métricas incluyendo un conjunto inicial de métricas y dimensiones que se utilizarán como base para supervisar una carga de trabajo. Con el tiempo, la carga de trabajo madura y puede agregar métricas y dimensiones adicionales para ayudarle a analizarla y respaldarla aún más. Las aplicaciones o cargas de trabajo pueden utilizar variasAWSrecursos y tener sus propias métricas personalizadas, debe agrupar estos recursos en un espacio de nombres para facilitar su identificación.

También debe considerar cómo se correlacionan los datos de registro y supervisión para poder identificar rápidamente los datos de registro y supervisión relevantes para diagnosticar problemas específicos. Puede usarLente de ServiceLens CloudWatchpara correlacionar rastros, métricas, registros y alarmas para diagnosticar problemas. También debe considerar la posibilidad de incluir dimensiones adicionales en métricas e identificadores en los registros de sus cargas de trabajo para ayudarle a buscar e identificar rápidamente problemas en todos los sistemas y servicios.

Uso de CloudWatch Alarmas para monitorear y alarmar

Puede usarAlarmas de CloudWatchpara reducir la supervisión manual de sus cargas de trabajo o aplicaciones. Comience revisando las métricas que está capturando para cada componente de carga de trabajo y determinar los umbrales adecuados para cada métrica. Asegúrese de identificar a qué miembros del equipo deben notificarse cuando se infringe un umbral. Debe establecer y dirigir grupos de distribución, en lugar de a miembros del equipo individuales.

Las alarmas de CloudWatch se pueden integrar con su solución de administración de servicios para crear automáticamente nuevos tickets y ejecutar flujos de trabajo operativos. Por ejemplo,AWSProporciona elAWSService Management Connector paraServiceNowyMesa de servicio de JiraPara ayudarle a configurar rápidamente las integraciones. Este enfoque es fundamental para garantizar que las alarmas elevadas se reconozcan y se alineen con los flujos de trabajo de operaciones existentes que podrían ya estar definidos en estos productos.

También puede crear varias alarmas para la misma métrica que tienen umbrales y períodos de evaluación diferentes, lo que ayuda a establecer un proceso de escalación. Por ejemplo, si tiene un`OrderQueueDepth`métrica que realiza un seguimiento de los pedidos de los clientes, puede definir un umbral inferior durante un breve período medio de un minuto que notifica a los miembros del equipo de aplicaciones por correo electrónico oSlack. También puede definir otra alarma para la misma métrica durante un período más largo de 15 minutos en el mismo umbral y esa página, correos electrónicos y notifica al equipo de aplicaciones y al jefe del equipo de aplicaciones. Por último, puede definir una tercera alarma para un umbral medio fijo durante un período de 30 minutos que notifica a la alta dirección y notifica a todos los miembros del equipo notificados previamente. Crear varias alarmas te ayuda a tomar diferentes acciones para diferentes condiciones. Puede comenzar con un sencillo proceso de notificación y, a continuación, ajustarlo y mejorarlo según sea necesario.

Uso de CloudWatch detección de anomalías para monitorear y alarma

Puede usarDetección de anomalías de Cloudsi no está seguro de los umbrales que se aplicarán a una métrica concreta o si desea que una alarma ajuste automáticamente los valores umbrales en función de los valores históricos observados. CloudWatch la detección de anomalías resulta especialmente útil para las métricas que pueden tener cambios regulares y predecibles en la actividad, por ejemplo, los pedidos de compra diarios para la entrega en el mismo día aumentan antes de un tiempo límite. La detección de anomalías permite umbrales que se ajustan automáticamente y pueden ayudar a reducir las falsas alarmas. Puede habilitar la detección de anomalías para cada métrica y estadística, y configurar CloudWatch alarma basada en valores atípicos.

Por ejemplo, puede habilitar la detección de anomalías para el`CPUUtilization`Métrica de y el`AVG`Estadística de una instancia EC2. La detección de anomalías utiliza hasta 14 días de datos históricos para crear el modelo de aprendizaje automático (ML). Puede crear varias alarmas con diferentes bandas de detección de anomalías para establecer un proceso de escalado de alarmas, similar a crear varias alarmas estándar con umbrales diferentes.

Para obtener más información acerca de esta sección, consulteCreación de una alarma de CloudWatch basada en la detección de anomalíasen la CloudWatch .

Alarmante en varias regiones y cuentas

Los propietarios de aplicaciones y cargas de trabajo deben crear alarmas a nivel de aplicación para cargas de trabajo que abarquen varias regiones. Recomendamos crear alarmas independientes en cada cuenta y región en la que se implementa la carga de trabajo. Puede simplificar y automatizar este proceso mediante el uso independiente de la cuenta y la región.AWS CloudFormation StackSets y plantillas para implementar recursos de aplicaciones con las alarmas necesarias. PlantillaPuede configurar las acciones de alarma para dirigirse a un tema común de Amazon Simple Notification Service (Amazon SNS), lo que significa que se utiliza la misma acción de notificación o corrección independientemente de la cuenta o región.

En entornos de varias cuentas y regiones, le recomendamos que cree alarmas agregadas para sus cuentas y regiones para supervisar los problemas de cuentas y regionales medianteAWS CloudFormation StackSets y métricas agregadas, como la media`CPUUtilization`En todas las instancias EC2.

También debe considerar la posibilidad de crear alarmas estándar para cada carga de trabajo configurada para el estándar. CloudWatch métricas y registros que captura. Por ejemplo, puede crear una alarma independiente para cada instancia de EC2 que monitoree la métrica de utilización de la CPU y notifica a un equipo de operaciones centrales cuando la utilización media de la CPU supera el 80% diariamente. También puede crear una alarma estándar que monitoree la utilización media de la CPU por debajo del 10% diariamente. Estas alarmas ayudan al equipo de operaciones centrales a trabajar con propietarios de cargas de trabajo específicos para cambiar el tamaño de las instancias de EC2 cuando sea necesario.

Automatizar la creación de alarmas con etiquetas de instancias EC2

Crear un conjunto estándar de alarmas para sus instancias EC2 puede llevar mucho tiempo, ser incoherente y propenso a errores. Puede acelerar el proceso de creación de alarmas utilizando elalarmas automáticas amazon-cloudwatchpara crear automáticamente un conjunto estándar de alarmas de CloudWatch para sus instancias EC2 y crear alarmas personalizadas basadas en etiquetas de instancia EC2. La solución elimina la necesidad de crear alarmas estándar manualmente y puede resultar útil durante una migración a gran escala de instancias de EC2 que utilizan herramientas como CloudEndure. También puede implementar esta solución conAWS CloudFormation StackSets Para admitir varias regiones y cuentas. Para obtener más información,

consulteUsar etiquetas para crear y mantener Amazon CloudWatch alarmas para instancias de Amazon EC2en elAWSBlog de.

Supervisión de la disponibilidad de aplicaciones y servicios

CloudWatch le ayuda a supervisar y analizar los aspectos de rendimiento y tiempo de ejecución de sus aplicaciones y cargas de trabajo. También debe supervisar los aspectos de disponibilidad y accesibilidad de sus aplicaciones y cargas de trabajo. Esto se puede lograr mediante el uso de un enfoque de monitoreo activo conControles de estado de Amazon Route 53yCloudWatch Synthetics.

Puede utilizar las comprobaciones de estado de Route 53 cuando desee supervisar la conectividad a una página web a través de HTTP o HTTPS, o la conectividad de red a través de TCP a un nombre o dirección IP públicos del sistema de nombres de dominio (DNS). Las comprobaciones de estado de Route 53 inician conexiones desde las regiones especificadas en intervalos de diez o 30 segundos. Puede elegir varias regiones en las que se ejecute la comprobación de estado, cada comprobación de estado se ejecuta de forma independiente y debe elegir al menos tres regiones. Puede buscar en el cuerpo de respuesta de una solicitud HTTP o HTTPS una subcadena específica si aparece en los primeros 5.120 bytes de datos devueltos para la evaluación de la comprobación de estado. Se considera que una solicitud HTTP o HTTPS se encuentra en buen estado si devuelve la respuesta 2xx o 3xx. Las comprobaciones de estado de Route 53 se pueden utilizar para crear una comprobación de estado compuesta comprobando el estado de otras comprobaciones de estado. Puede hacerlo si tiene varios endpoints de servicio y desea realizar la misma notificación cuando uno de ellos se vuelve inestable. Si utiliza Route 53 para DNS, puede configurar Route 53 paraconmutación por error en otra entrada DNSsi una comprobación de estado se vuelve poco saludable. Para cada carga de trabajo crítica, debe considerar la posibilidad de configurar comprobaciones de estado de Route 53 para endpoints externos que son críticos para las operaciones normales. Las comprobaciones de estado de Route 53 pueden ayudarlo a evitar escribir lógica de conmutación por error en sus aplicaciones.

Los sintéticos CloudWatch le permiten definir un canario como un script para evaluar el estado y la disponibilidad de sus cargas de trabajo. Los canaries son scripts escritos en Node.js o en Python y funcionan mediante protocolos HTTP o HTTPS. Crean funciones de Lambda en la cuenta, que usan Node.js como marco. Cada canario que defina puede realizar varias llamadas HTTP o HTTPS a distintos endpoints. Esto significa que puede supervisar el estado de una serie de pasos, como un caso de uso o un endpoint con dependencias descendentes. Canaries crean CloudWatch métricas que incluyen cada paso que se ha ejecutado para que puedas alarmar y medir diferentes pasos de forma independiente. Aunque los canarios requieren más planificación y esfuerzo para desarrollar que los controles de estado de Route 53, le proporcionan un enfoque de monitoreo y evaluación altamente personalizable. Canaries también admite recursos privados que se ejecutan dentro de la

nube privada virtual (VPC), lo que los hace ideales para la supervisión de la disponibilidad cuando no tiene una dirección IP pública para el endpoint. También puede utilizar canarios para supervisar las cargas de trabajo locales siempre que tenga conectividad desde la VPC hasta el punto final. Esto es especialmente importante cuando tiene una carga de trabajo que incluye endpoints que existen en las instalaciones.

Aplicaciones de rastreo conAWS X-Ray

Una solicitud a través de su aplicación puede consistir en llamadas a bases de datos, aplicaciones y servicios web que se ejecutan en servidores locales, Amazon EC2, contenedores o Lambda. Al implementar el seguimiento de aplicaciones, puede identificar rápidamente la causa raíz de los problemas en las aplicaciones que utilizan componentes y servicios distribuidos. Puede usarAWS X-Raypara realizar un seguimiento de las solicitudes de aplicación en varios componentes. Muestras de X-Ray y visualiza las solicitudes en unGráfico de servicioscuando fluyen a través de los componentes de la aplicación y cada componente se representa como un segmento. X-Ray genera identificadores de seguimiento para que pueda correlacionar una solicitud cuando fluye a través de varios componentes, lo que le ayuda a ver la solicitud de extremo a extremo. Puede mejorarlo aún más si incluye anotaciones y metadatos para ayudar a buscar e identificar de forma exclusiva las características de una solicitud.

Le recomendamos que configure e instrumente cada servidor o punto final de su aplicación con X-Ray. X-Ray se implementa en el código de su aplicación realizando llamadas al servicio X-Ray. X-Ray también proporcionaAWSSDK para varios idiomas, incluidos clientes instrumentados que envían datos automáticamente a X-Ray. Los SDK de X-Ray proporcionan parches a las bibliotecas comunes utilizadas para realizar llamadas a otros servicios (por ejemplo, HTTP, MySQL, PostgreSQL o MongoDB).

X-Ray proporciona un demonio de rayos X que puede instalar y ejecutar en Amazon EC2 y Amazon ECS para transmitir datos a X-Ray. X-Ray crea seguimientos para su aplicación que capturan datos de rendimiento de los servidores y contenedores que ejecutan el demonio X-Ray que atendió la solicitud. X-Ray instrumenta automáticamente tus llamadas aAWSservicios, como Amazon DynamoDB, como subsegmentos mediante la aplicación de parchesAWSSDK. X-Ray también se puede integrar automáticamente con las funciones de Lambda.

Si los componentes de la aplicación realizan llamadas a servicios externos que no pueden configurar e instalar el daemon X-Ray o instrumentar el código, puede crearsubsegmentos para empaquetar llamadas a servicios externos. Se correlaciona con X-Ray CloudWatch registros y métricas con los seguimientos de la aplicación si está utilizando elAWS X-Ray SDK para Java, lo que significa que puede analizar rápidamente las métricas y los registros relacionados para las solicitudes.

Implementación de daemon X-Ray para rastrear aplicaciones y servicios en Amazon EC2

Debe instalar y ejecutar el daemon X-Ray en las instancias de EC2 en las que se ejecutan los componentes de la aplicación o los microservicios. Puede usar unScript de datos de usuariopara implementar el demonio de X-Ray cuando se aprovisionan instancias EC2 o puede incluirlo en el proceso de compilación de AMI si crea sus propias AMI. Esto puede resultar especialmente útil cuando las instancias EC2 son efímeras.

Debe utilizar State Manager para asegurarse de que el demonio de X-Ray esté instalado de forma coherente en las instancias EC2. Para Amazon EC2Windowsinstancias, puede utilizar Systems ManagerAWS-Ejecute un documento de PowerShellScriptpara ejecutar laScript de Windowsque descarga e instala el agente X-Ray. Para las instancias EC2 en Linux, puede utilizar elAWS-RunShellScript documento para ejecutar el script Linux quedescarga e instala el agente como servicio.

Puede utilizar el Systems ManagerAWS-Ejecute un documento de Remote Scriptpara ejecutar el script en un entorno de varias cuentas. Debe crear un bucket de S3 al que se pueda acceder desde todas sus cuentas y le recomendamoscreación de un bucket de S3 con una política de bucket basada en la organizaciónsi utilizaAWS Organizations. A continuación, cargue los scripts en el bucket de S3 pero asegúrese de que el rol de IAM de sus instancias EC2 tenga permiso para acceder al bucket y a los scripts.

También puede configurar State Manager para asociar los scripts a instancias EC2 que tienen instalado el agente X-Ray. Debido a que es posible que todas las instancias de EC2 no requieran ni utilicen X-Ray, puede dirigirse a la asociación con etiquetas de instancia. Por ejemplo, puede crear la asociación de State Manager en función de la presencia de`InstallAWSXRayDaemonWindows`o`InstallAWSXRayDaemonLinux`etiquetas.

Implementación de daemon X-Ray para rastrear aplicaciones y servicios en Amazon ECS o Amazon EKS

Puede desplegar elDemonio X-Raycomo contenedor sidecar para cargas de trabajo basadas en contenedores como Amazon ECS o Amazon EKS. Los contenedores de aplicaciones se pueden conectar a su contenedor sidecar con vinculación de contenedores si utiliza Amazon ECS, o el contenedor puede conectarse directamente al contenedor sidecar en localhost si utilizaModo de red awsvpc.

Para Amazon EKS, puede definir el demonio X-Ray en la definición de pod de la aplicación y, a continuación, la aplicación puede conectarse al daemon a través del host local en el puerto del contenedor que especificó.

Configuración de Lambda para rastrear solicitudes en X-Ray

Es posible que la aplicación incluya llamadas a funciones de Lambda. No es necesario instalar el daemon X-Ray para Lambda porque el proceso del daemon es totalmente administrado por Lambda y el usuario no puede configurarlo. Puede habilitarlo para su función Lambda utilizando elAWS Management Consoley verificando laActive tracingen la consola X-Ray.

Para realizar una instrumentación adicional, puede agrupar el SDK de X-Ray con su función Lambda para registrar las llamadas salientes y añadir anotaciones o metadatos.

Implementación de aplicaciones para X-Ray

Debe evaluar el SDK de X-Ray que se alinea con el lenguaje de programación de la aplicación y clasificar todas las llamadas que realiza su aplicación a otros sistemas. Revise los clientes proporcionados por la biblioteca que eligió y compruebe si el SDK puede instrumentar automáticamente el seguimiento de la solicitud o respuesta de la aplicación. Determine si los clientes proporcionados por el SDK se pueden utilizar para otros sistemas posteriores. Para los sistemas externos a los que llama su aplicación y que no puede instrumentar con X-Ray, debe crear subsegmentos personalizados para capturarlos e identificarlos en la información de seguimiento.

Cuando instruye su aplicación, asegúrese de crear anotaciones para ayudarlo a identificar y buscar solicitudes. Por ejemplo, la aplicación podría utilizar un identificador para los clientes, como`customer id`o segmentar distintos usuarios en función de su función en la aplicación.

Puede crear un máximo de 50 anotaciones para cada seguimiento, pero puede crear un objeto de metadatos que contenga uno o más campos siempre que el documento de segmento no supere los 64 kilobytes. Debe utilizar anotaciones de forma selectiva para localizar información y utilizar el objeto de metadatos para proporcionar más contexto que ayude a solucionar los problemas de la solicitud una vez localizada.

Configuración de las reglas de muestreo de X-Ray

Porpersonalización de reglas de muestreo, puede controlar la cantidad de datos que va a registrar y modificar el comportamiento de muestreo sin modificar ni volver a implementar su código. Las

reglas de muestreo indican al SDK de X-Ray el número de solicitudes que va a registrar para un conjunto de criterios. De forma predeterminada, el SDK de X-Ray SDK dela primera solicitud cada segundo y el cinco por ciento de cualquier solicitud adicional. Una petición por segundo es el depósito. Esto garantiza que se registre al menos un registro de seguimiento cada segundo mientras el servicio atienda solicitudes. El cinco por ciento es el porcentaje al que se muestrean las solicitudes adicionales más allá del tamaño del depósito.

Debe revisar y actualizar la configuración predeterminada para determinar un valor adecuado para su cuenta. Los requisitos pueden variar en entornos de desarrollo, pruebas, pruebas de rendimiento y producción. Es posible que tengas aplicaciones que requieran sus propias reglas de muestreo en función de la cantidad de tráfico que reciben o de su nivel de criticidad. Debe comenzar con una línea de base y volver a evaluar periódicamente si la línea de base cumple con sus requisitos.

Paneles y visualizaciones con CloudWatch

Los paneles le ayudan a centrarse rápidamente en las áreas que preocupan a las aplicaciones y las cargas de trabajo. CloudWatch proporciona paneles automáticos y también puede crear fácilmente paneles que utilicen CloudWatch Métricas de . CloudWatch los paneles proporcionan más información que ver métricas de forma aislada porque le ayudan a correlacionar varias métricas e identificar tendencias. Por ejemplo, un panel que incluye pedidos recibidos, memoria, utilización de CPU y conexiones de bases de datos puede ayudarle a correlacionar los cambios en las métricas de cargas de trabajo en variosAWSrecursos mientras el recuento de pedidos aumenta o disminuye.

Debe crear paneles a nivel de cuenta y aplicación para supervisar las cargas de trabajo y las aplicaciones. Puede comenzar con CloudWatch paneles automáticos, que sonAWSpaneles de nivel de servicio preconfigurados con métricas específicas de servicio. Los paneles de servicio automáticos muestran todos los estándares CloudWatch métricas para el servicio. Los paneles automáticos trafican todos los recursos utilizados para cada métrica de servicio y le ayudan a identificar rápidamente los recursos atípicos de su cuenta. Esto puede ayudarle a identificar recursos con alta y baja utilización, lo que puede ayudarle a optimizar sus costos.

Creación de paneles de servicio cruzado

Puede crear paneles de varios servicios si ve el panel de nivel de servicio automático para unAWSservicio y uso delAdd to dashboardopción de laActionsmenú. A continuación, puede agregar métricas de otros paneles automáticos al nuevo panel y eliminar métricas para limitar el enfoque del panel. También debe agregar sus propias métricas personalizadas para realizar un seguimiento de las observaciones clave (por ejemplo, pedidos recibidos o transacciones por segundo). Crear su propio panel de control multiservicio personalizado le ayuda a centrarse en las métricas más relevantes para su carga de trabajo. Le recomendamos que cree paneles de control multiservicio a nivel de cuenta que cubran métricas clave y muestren todas las cargas de trabajo de una cuenta.

Si tiene un espacio de oficina central o un área común para sus equipos de operaciones en la nube, puede mostrar el CloudWatch panel de control en un monitor de TV grande en modo de pantalla completa con actualización automática.

Creación de paneles específicos de aplicaciones o cargas de trabajo

Le recomendamos que cree paneles específicos de aplicaciones y cargas de trabajo que se centren en métricas y recursos clave para cada aplicación o carga de trabajo crítica de su entorno de producción. Los paneles específicos de la aplicación y la carga de trabajo se centran en las métricas personalizadas de la aplicación o la carga de trabajo e importantesAWSmétricas de recursos que influyen en su rendimiento.

Debe evaluar y personalizar periódicamente su CloudWatch paneles de aplicaciones o cargas de trabajo para realizar un seguimiento de las métricas clave después de que se produzcan incidentes. También debe actualizar los paneles específicos de la aplicación o de la carga de trabajo cuando se introducen o retiren las funciones. Las actualizaciones de la carga de trabajo y los paneles específicos de la aplicación deben ser una actividad obligatoria para mejorar continuamente la calidad, además del registro y la supervisión.

Creación de paneles de cuentas y Regiones cruzadas

AWSlos recursos son principalmente regionales y las métricas, alarmas y tableros son específicos de la región en la que se implementan los recursos. Esto puede requerir que cambie de regiones para ver métricas, paneles y alarmas de cargas de trabajo y aplicaciones entre regiones. Si separas las aplicaciones y las cargas de trabajo en varias cuentas, es posible que también tengas que volver a autenticarte e iniciar sesión en cada cuenta. Sin embargo, CloudWatch admite la visualización de datos entre cuentas y regiones desde una única cuenta, lo que significa que puede ver métricas, alarmas, paneles de mando y widgets de registro en una sola cuenta y región. Esto resulta muy útil si tiene una cuenta de registro y supervisión centralizada.

Los propietarios de cuentas y los propietarios de equipos de aplicaciones deben crear paneles para aplicaciones de varias regiones específicas de la cuenta para supervisar eficazmente las métricas clave en una ubicación centralizada. Los paneles de CloudWatch admiten automáticamente los widgets entre regiones, lo que significa que puede crear un panel que incluya métricas de varias regiones sin necesidad de configuración adicional.

Una excepción importante es la CloudWatch Widget Logs Insights porque los datos de registro solo se pueden mostrar para la cuenta y la región en la que ha iniciado sesión actualmente. Puede crear métricas específicas de cada región a partir de sus registros mediante filtros de métricas y estas

métricas se pueden mostrar en un panel de control entre regiones. A continuación, puede cambiar a la región específica cuando necesite analizar más a fondo esos registros.

Los equipos de operaciones deben crear un panel centralizado que supervise las métricas importantes entre cuentas y regiones. Por ejemplo, puede crear un panel multicuenta que incluya la utilización agregada de CPU en cada cuenta y región. También puede utilizarCrecimiento de métricaspara agregar datos y paneles entre varias cuentas y Regiones.

Uso de matemáticas métricas para ajustar la observabilidad y alarmante

Puede utilizar matemáticas métricas para ayudar a calcular las métricas en formatos y expresiones relevantes para sus cargas de trabajo. Las métricas calculadas se pueden guardar y ver en un panel con fines de seguimiento. Por ejemplo, las métricas de volumen estándar de Amazon EBS proporcionan el número de lecturas (`VolumeReadOps`) y escribe (`VolumeWriteOps`) operaciones realizadas durante un período específico.

Sin embargo,AWSproporciona directrices sobre el rendimiento del volumen de Amazon EBS en IOPS. Puede graficar y calcular las IOPS de su volumen de Amazon EBS en matemáticas métricas añadiendo la`VolumeReadOps`y`VolumeWriteOps`y luego dividir por el período elegido para estas métricas.

En este ejemplo, resumimos las IOPS en el período y luego dividimos por la duración del período para obtener las IOPS. A continuación, puede configurar una alarma contra esta expresión matemática métrica para avisarle cuando la IOPS de su volumen se aproxima a la capacidad máxima para su tipo de volumen. Para obtener más información y ejemplos sobre el uso de cálculos de métricas para supervisar sistemas de archivos Amazon Elastic File System (Amazon EFS) con CloudWatch métricas, consulteAmazon CloudWatch metric math simplifica la supervisión casi en tiempo real de sus sistemas de archivos Amazon EFS y másen elAWSBlog de.

Uso de paneles automáticos para Amazon ECS, Amazon EKS y Lambda con CloudWatchContainer Conocimientos y CloudWatch Conocimientos de Lambda

CloudWatch Container Insights crea paneles dinámicos y automáticos para cargas de trabajo de contenedores que se ejecutan en Amazon ECS y Amazon EKS. Debe habilitar Container

Insights para que tenga observabilidad de la CPU, la memoria, el disco, la red y la información de diagnóstico, como errores de reinicio del contenedor. Container Insights genera paneles dinámicos que puede filtrar rápidamente en los niveles de clúster, instancia de contenedor o nodo, servicio, tarea, pod y contenedor individual. Container Insightsse configura a nivel de clúster y nodo o instancia de contenedorsegún el valor deAWSservicio de.

Similar a Container Insights, CloudWatch Lambda Insights crea paneles dinámicos y automáticos para sus funciones de Lambda. Esta solución recopila, agrega y resume métricas a nivel de sistema, incluido el tiempo de CPU, la memoria, el disco y el uso de red. También recopila, agrega y resume información de diagnóstico como inicios en frío y paradas de trabajo de Lambda para ayudarle a aislar y resolver rápidamente problemas con las funciones de Lambda. Lambda está habilitado a nivel de función y no requiere ningún agente.

Container Insights y Lambda Insights también le ayudan a cambiar rápidamente a los registros de aplicaciones o de rendimiento, seguimientos de X-Ray y un mapa de servicios para visualizar las cargas de trabajo de contenedores. Ambos usan el CloudWatch formato de métricas integradas para capturar CloudWatch métricas y registros de rendimiento.

Puedes crear un recurso compartido CloudWatch panel de su carga de trabajo que utiliza las métricas capturadas por Container Insights y Lambda Insights. Para ello, puede filtrar y ver el panel automático a través de CloudWatch Container Insights y, a continuación, elegir elAgregar al panelque le permite agregar las métricas mostradas a un panel de CloudWatch estándar. A continuación, puedes eliminar o personalizar las métricas y añadir otras métricas para representar correctamente tu carga de trabajo.

Integración con CloudWatchAWSServicios de

AWSproporciona muchos servicios que incluyen opciones de configuración adicionales para registros y métricas. Estos servicios a menudo le permiten configurar CloudWatch Registros para la salida de registros y CloudWatch métricas para la salida de métricas. La infraestructura subyacente utilizada para proporcionar estos servicios está gestionada porAWSyes inaccesible, pero puede utilizar las opciones de registro y métricas de los servicios aprovisionados para obtener más información y solucionar problemas. Por ejemplo, puede hacer publicacionesLogs de flujo de VPC a CloudWatch, o también puedesconfigurar instancias de Amazon Relational Database Service (Amazon RDS) para publicar registros en CloudWatch.

MásAWSLos servicios registran sus llamadas a la API conIntegración de aAWS CloudTrail. CloudTrail tambiénadmite la integración con . CloudWatch Registrosy esto significa que puedes buscar y analizar la actividad enAWSServicios de . También puede utilizar Amazon CloudWatch Eventos de Amazon EventBridge para crear y configurar automatización y notificaciones con CloudWatch Reglas de eventos de eventos para acciones específicas realizadas enAWSServicios de . Ciertos serviciosIntegración de directamentecon CloudWatch Eventos y EventBridge. También puedecrear eventos entregados mediante CloudTrail.

Amazon Managed Grafana para paneles y visualización

Amazon Managed Grafanase puede utilizar para observar y visualizar suAWScargas de trabajo. Amazon Managed Grafana le ayuda a visualizar y analizar sus datos operativos a escala. Grafanaes una plataforma de análisis de código abierto que le ayuda a consultar, visualizar, alertar y comprender sus métricas dondequiera que estén almacenadas. Amazon Managed Grafana es particularmente útil si su organización ya utiliza Grafana para la visualización de las cargas de trabajo existentes y desea ampliar la cobertura aAWScargas de trabajo. Puede utilizar Amazon Managed Grafana con CloudWatch poragregarlo como fuente de datos, lo que significa que puede crear visualizaciones mediante CloudWatchMétricas de . Amazon Managed Grafana admiteAWS Organizationsy puede centralizar los paneles mediante CloudWatch Métricas de varias cuentas y regiones.

La siguiente tabla proporciona las ventajas y consideraciones para usar Amazon Managed Grafana en lugar de CloudWatch para el panel de. Un enfoque híbrido podría ser adecuado en función de los diferentes requisitos de los usuarios finales, las cargas de trabajo y las aplicaciones.

Cree visualizaciones y paneles que se integren con fuentes de datos compatibles con Amazon Managed Grafana y Grafana de código abierto	Amazon Managed Grafana le ayuda a crear visualizaciones y paneles a partir de muchas fuentes de datos diferentes, entre las que se incluyen CloudWatch Métricas de . Amazon Managed Grafana incluye una serie de fuentes de datos integradas que abarcanAWSservicios, software de código abierto y software COTS. Para obtener más información acerca de este tema, consulteFuentes de datos integradas en la documentación de Amazon Managed Grafana. También puede añadir soporte para más fuentes de datos actualizando su espacio de trabajo aGrafana Enterprise. Grafana también apoyacomplementos de origen de datosque permiten comunicarse con diferentes sistemas externos. CloudWatchLos paneles de requieren CloudWatch Métrica o CloudWatch Consulta de Logs Insights para que los datos

	que se muestren se muestran en un CloudWatch Panel de.
Administre el acceso a su solución de paneles por separado de suAWSAcceso a la cuenta	Amazon Managed Grafana requiere el uso deAWS IAM Identity Center(Centro de identidad de IAM) yAWS Organizationspara la autenticación y la autorización. Esto le permite autenticar a los usuarios en Grafana mediante el uso de la federación de identidades que puede que ya utilice con IAM Identity Center oAWS Organizations. Sin embargo, si no utiliza el Centro de identidad de IAM oAWS Organizations, se configura como parte del proceso de configuración de Amazon Managed Grafana. Esto podría convertirse en un problema si su organización ha limitado el uso de IAM Identity Center oAWS Organizations.
Ingiera datos y acceda a ellos en varias cuentas y regiones conAWS Organizationsintegración	Amazon Managed Grafana se integra conAWS Organizationspara permitirle leer datos deAWSfuentes como CloudWatch y Amazon OpenSearch Servicio en todas tus cuentas. Esto permite crear paneles de control que muestren visualizaciones con datos en todas sus cuentas. Para habilitar automáticamente el acceso a los datos enAWS Organizations, debe configurar su espacio de trabajo Amazon Managed Grafana en laAWS Organizationscuenta de administración. Esto no se recomienda en función deAWS Organizationsprácticas recomendadas para la cuenta de administración. En cambio, CloudWatch también admite paneles para cuentas y Regiones cruzadas para CloudWatch Métricas de.

Utilice widgets de visualización avanzados y definiciones de Grafana disponibles en la comunidad de código abierto	Grafana proporciona una gran colección de visualizaciones que puede usar al crear sus paneles. También hay una gran biblioteca de paneles aportados por la comunidad que puede editar y reutilizar de acuerdo con sus requisitos.
Utilice paneles de control con implement aciones de Grafana nuevas y existentes	Si ya usa Grafana, puede importar y exportar paneles de sus implementaciones de Grafana y personalizarlos para usarlos en Amazon Managed Grafana. Amazon Managed Grafana le permite estandarizar Grafana como su solución de paneles.
Configuración y configuración avanzadas para espacios de trabajo, permisos y fuentes de datos	Amazon Managed Grafana le permite crear varios espacios de trabajo de Grafana que tienen su propio conjunto de fuentes de datos, usuarios y políticas configurados. Esto puede ayudarlo a cumplir con los requisitos de casos de uso más avanzados, así como con configura ciones de seguridad avanzadas. Las capacidad es avanzadas pueden requerir que sus equipos aumenten su experiencia con Grafana si aún no tienen estas habilidades.

Diseño e implementación de registros y monitorización con CloudWatch PREGUNTAS FRECUENTES

En esta sección se proporcionan respuestas a preguntas frecuentes sobre el diseño e implementación de una solución de registro y supervisión con CloudWatch.

¿Dónde guardo mi CloudWatch archivos de configuración?

La CloudWatch agent for Amazon EC2 puede aplicar varios archivos de configuración que se almacenan en el CloudWatch directorio de configuración. Idealmente, debería almacenar la configuración de CloudWatch como un conjunto de archivos porque puede controlar las versiones y utilizarlos de nuevo en varias cuentas y entornos. Para obtener más información acerca de este tema, consulteAdministrar CloudWatch las configuracionessección de esta guía. Alternativamente, puede almacenar los archivos de configuración en un repositorio en GitHub y automatice la recuperación de los archivos de configuración cuando se aprovisiona una nueva instancia EC2.

¿Cómo puedo crear un ticket en mi solución de administración de servicios cuando se activa una alarma?

Integra el sistema de administración de servicios con un tema de Amazon Simple Notification Service (Amazon SNS) y configura el CloudWatch alarma para notificar al tema de SNS cuando se activa una alarma. El sistema integrado recibe el mensaje SNS y puede crear un ticket mediante las API o SDK de los sistemas de administración de servicios.

¿Cómo puedo usar? CloudWatch para capturar archivos de registro en mis contenedores?

Las tareas de Amazon ECS y los pods de Amazon EKS se pueden configurar para enviar automáticamente los resultados STDOUT y STDERR a CloudWatch. El enfoque recomendado para registrar aplicaciones en contenedores es hacer que los contenedores envíen su salida a STDOUT y STDERR. Esto también se trata en elManifiesto de la aplicación de doce factores.

Sin embargo, si desea enviar archivos de registro específicos a CloudWatch a continuación, puede montar un volumen en su pod de Amazon EKS o en la definición de tarea de Amazon ECS en el que

la aplicación escribirá sus archivos de lote y utilizará un contenedor sidecar para Fluentd o Fluent Bit para enviar los registros a CloudWatch. Debe considerar la posibilidad de vincular simbólicamente un archivo de registro específico de su contenedor a`/dev/stdouty/dev/stderr`. Para obtener más información acerca de este tema, consulteVer registros de un contenedor o servicioen la documentación de Docker.

¿Cómo puedo supervisar los problemas de salud paraAWSservicios?

Puede utilizar elAWS Health Dashboardmonitorear AWSeventos de estado. También puede consultar elaws-health-tools GitHub repositorio para soluciones de automatización de muestras relacionadas conAWSeventos de estado.

¿Cómo puedo crear un personalizado CloudWatch métrica cuando no existe soporte de agente?

Puede utilizar el formato de métricas integradas para incorporar métricas en CloudWatch. También puede utilizarAWSSDK (por ejemplo,put_metric_data),AWS CLI(por ejemplo,put-metric-data), oAWSAPI (por ejemplo,PutMetricData) para crear métricas de personalizadas. Debe considerar cómo se mantendrá cualquier lógica personalizada a largo plazo. Un enfoque sería utilizar Lambda con soporte de formato métrico integrado integrado para crear sus métricas, junto con un CloudWatch Evento de eventosregla de programaciónpara establecer el período de la métrica.

¿Cómo puedo integrar mis herramientas de registro y supervisión existentes conAWS?

Debe consultar la guía proporcionada por el proveedor de software o servicio para integrarse conAWS. Es posible que puedas utilizar el software del agente, el SDK o una API proporcionada para enviar registros y métricas a su solución. También podría utilizar una solución de código abierto, como Fluentd o Fluent Bit, configurada según las especificaciones del proveedor. También puede utilizar laAWSSDK y CloudWatch Registra filtros de suscripción con Lambda y Kinesis Data Streams para crear procesadores de registros y remitentes personalizados. Por último, también debe considerar cómo integrará el software si utiliza varias cuentas y regiones.

Recursos

Introducción

- AWSWell-Architected

Resultados comerciales específicos

- logging-monitoring-apg-guide-ejemplos
- Seis ventajas de la computación en nube

Planificación de su CloudWatch despliegue

- Terminología y conceptos de AWS Organizations
- AWS Systems ManagerConfiguración rápida
- Recopilación de métricas y registros de instancias Amazon EC2 y servidores en los servidores en las instalaciones con el CloudWatch agente
- cloudwatch-config-s3 cubos. yaml
- Cree el archivo de configuración del CloudWatch agente con el asistente
- Empresa DevOps: por qué debe ejecutar lo que crea
- Exportación de datos de registro a Amazon S3
- Control de acceso detallado en Amazon OpenSearch Service
- Cuotas de Lambda
- Cree o edite de forma manual el archivo de configuración del CloudWatch agente
- Procesamiento en tiempo real de datos de registros con suscripciones
- Herramientas sobre las que construirAWS

Configuración del CloudWatch agente para instancias EC2 y servidores en las instalaciones

- Dimensiones de Amazon EC2

- Instancias de rendimiento ampliable
- CloudWatch conjuntos predefinidos de métricas del agente
- Recopilación de métricas de procesos con el complemento procstat
- Configuración del CloudWatch agente para procstat
- Activar o desactivar el monitoreo detallado para las instancias
- Incorporación de registros de alta cardinalidad y generación de métricas con formato de métrica CloudWatch integrada
- Uso de grupos de registros y flujos de registro
- Mostrar las CloudWatch métricas de disponibles para las instancias
- PutLogEvents
- Recuperación de las métricas personalizadas con collectd
- Recuperación de las métricas personalizadas con StatsD

CloudWatch enfoques de instalación de agentes para Amazon EC2 y servidores locales

- Creación de un rol de servicio de IAM para un entorno híbrido
- Cree una activación de instancia administrada para un entorno híbrido
- Cree roles y usuarios de IAM para utilizarlos con el CloudWatch agente
- Descargue y configure el CloudWatch agente con la línea de comandos
- ¿Cómo puedo configurar los servidores locales que utilizan el agente de Systems Manager y el CloudWatch agente unificado para que usen solo credenciales temporales?
- Requisitos previos para las operaciones con conjuntos de pilas
- Uso de instancias puntuales

Registro y monitoreo en Amazon ECS

- amazon-cloudwatch-logs-for-bit fluido
- CloudWatch Métricas de Amazon ECS
- Métricas de Container Insights

- Agente de contenedor de Amazon ECS
- Tipos de lanzamiento de Amazon ECS
- Implementación del CloudWatch agente para recopilar métricas de nivel de instancia EC2 en Amazon ECS
- ecs_cluster_con_cloudwatch_linux.yaml
- Ejemplo de ecs_cw_emf
- Ejemplo de ecs_firelense_emf
- ecs-task-nginx-firelense.json
- Recuperación de metadatos de AMI optimizados para Amazon ECS
- Uso del controlador de registros awslogs
- Uso de las bibliotecas de cliente para generar registros de formato de métricas integradas

Registro y monitoreo en Amazon EKS

- Registro de plano de control de Amazon EKS
- amazon_eks_managed_node_group_launch_config.yaml
- Nodos de Amazon EKS
- amazon-eks-nodegroup.yaml
- Acuerdo de nivel de servicio de Amazon EKS
- Monitoreo de métricas de Container Insights Prometheus
- Controla las métricas del plano con Prometheus
- Implementar el panel de Kubernetes (interfaz de usuario web)
- Registro Fargate fragmentación
- Fluent Bit para Amazon EKS en Fargate
- Cómo capturar los registros de aplicaciones cuando se utiliza Amazon EKS en Fargate
- Instalación del CloudWatch agente para recopilar métricas de Prometheus
- Instalación del servidor de métricas de Kubernetes
- kubernetes /panel
- Escalador automático de módulos horizontales de Kubernetes
- Componentes del plano de control de Kubernetes

- Módulos de Kubernetes
- Compatibilidad con las plantillas de lanzamiento
- Grupos de nodos administrados
- Comportamiento de actualización de nodos gestionados
- servidor de métricas
- Monitorización de Amazon EKS en Fargate mediante Prometheus y Grafana
- prometheus_jmx
- prometheus/jmx_export
- El raspado de fuentes de Prometheus adicionales y la importación de tales métricas
- Nodos autoadministrados
- Enviar registros a CloudWatch Logs
- Configure FluentD como un DaemonSet para enviar CloudWatch registros a Logs
- Configure la carga de trabajo de muestra de Java/JMX en Amazon EKS y Kubernetes
- Tutorial para añadir un nuevo destino de raspado de Prometheus: métricas del servidor de la API de Prometheus
- Escalador automático vertical de pods

Registro y métricas paraAWS Lambda

- Errores de invocación de Lambda
- registro: función de registro para Python
- Uso de las bibliotecas de cliente para generar registros de formato de métricas integradas
- Uso de métricas de funciones de Lambda

Búsqueda y análisis de registros CloudWatch

- La familia Beats
- Logstash elástico
- Pila elástica
- Transmisión de datos de CloudWatch registros a Amazon OpenSearch Service

Opciones alarmantes con CloudWatch

- amazon-cloudwatch-auto-alarms
- AWSConector de administración de servicios para Jira Service Management
- AWSConector de administración de servicios para ServiceNow

Supervisión de la disponibilidad de aplicaciones y servicios

- Configuración de la recuperación ante errores a nivel de DNS

Aplicaciones de rastreo conAWS X-Ray

- Integración en red de las tareas Amazon ECS
- Configuración de reglas de muestreo en la consola de X-Ray
- Ejecute PowerShell comandos o scripts de Windows
- Ejecución del daemon X-Ray en Amazon EC2
- Envío de datos de seguimiento a X-Ray
- Gráfico de servicio en X-Ray

Tableros y visualizaciones con CloudWatch

- Amazon CloudWatch Metric Math simplifica la supervisión casi en tiempo real de sus sistemas de archivos Amazon EFS
- Configuración de CloudWatch Container Insights
- Uso de matemáticas en las métricas

CloudWatch integración conAWS servicios

- Servicios e integraciones compatibles con AWS CloudTrail
- CloudWatch Ejemplos de eventos de servicios compatibles
- Eventos entregados a través de CloudTrail
- Monitorización de archivos de CloudTrail registro con CloudWatch registros

- Publicación de registros del motor de base de datos en CloudWatch Logs
- Publicación de registros de flujo en CloudWatch Logs

Grafana gestionado por Amazon para paneles y visualización

- Prácticas recomendadas para la cuenta de administración enAWS Organizations
- Fuentes de datos integradas para Amazon Managed Grafana
- Tableros multicuentas y entre regiones en CloudWatch
- Plugins de Grafana

Historial de documentos

En la siguiente tabla se describen los cambios importantes de esta guía. Si quieres recibir notificaciones sobre future actualizaciones, puedes suscribirte a una fuente RSS.

Cambio	Descripción	Fecha
Información de registro actualizada	Se actualizó la sección sobre el registro deAWS Lambda.	17 de abril de 2023
Información de configuración actualizada	Se actualizó y cambió el nombre de la sección sobre la creación y el almacenamiento de CloudWatch configuraciones.	9 de febrero de 2023
Información de métricas actualizada	Se actualizó la información de métricas personalizadas de la aplicación en la sección Métricas de Amazon ECS.	31 de enero de 2023
Avisos de vista previa eliminados	Grafana de Amazon ya está disponible con carácter general.	25 de mayo de 2022
Sección eliminada	CloudWatch Las métricas de SDK ya no son compatibles.	7 de enero de 2022
Publicación inicial	—	30 de abril de 2021

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 la base de datos de Oracle en las instalaciones a Amazon Aurora PostgreSQL-Compatible Edition.
- 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 in the Cloud. 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 el sistema de administración de las 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 en la nube. 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. Este escenario de migración es específico de VMware Cloud on AWS, que admite la compatibilidad de máquinas virtuales (VM) y la portabilidad de las cargas de trabajo entre su entorno local y. AWS Puede utilizar las tecnologías de VMware Cloud Foundation desde los centros de datos en las instalaciones al migrar una infraestructura a VMware Cloud en AWS. Ejemplo: traslade el hipervisor que aloja su base de datos de Oracle a VMware Cloud on. 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 el 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 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 empresarial en la AWS nube.

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 la AWS nube:

- 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 AWS Cloud 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 una administración y un 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 deriva

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 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 keyloggers.

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 la migración a la nube. 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 la AWS nube. 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 la 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 del 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 y es 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, consulte la documentación de Secret in the 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. Existen cuatro tipos principales de controles de seguridad: preventivos, de detección, con capacidad 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.