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

Introducción 1
Resultados empresariales específicos 5
Acelere la preparación operativa 5
Mejore la excelencia operativa 5
Mejore la visibilidad operativa 6
Amplíe las operaciones y reduzca los gastos generales 6
Planificación de la CloudWatch implementación 7
Utilización CloudWatch en cuentas centralizadas o distribuidas 8
Administrar los archivos CloudWatch de configuración de los agentes 11
Administrar CloudWatch las configuraciones 12
Ejemplo: almacenar los archivos CloudWatch de configuración en un bucket de S3 15
Configuración del CloudWatch agente para las instancias EC2 y los servidores locales 17
Configuración del agente CloudWatch 17
Configuración de la captura de registros para instancias EC2 18
Configuración de la captura de métricas para instancias EC2 20
Configuración a nivel de sistema CloudWatch 23
Configuración de registros a nivel de sistema 23
Configurar métricas a nivel de sistema 26
Configuración a nivel de aplicación CloudWatch 26
Configurar los registros a nivel de aplicación 27
Configuración de métricas a nivel de aplicación 28
CloudWatch enfoques de instalación de agentes para Amazon EC2 y servidores locales 30
Instalación del CloudWatch agente mediante Systems Manager Distributor y State Manager 30
Configure State Manager y Distributor para el despliegue y la configuración de los CloudWatch agentes 32
Utilice la configuración rápida de Systems Manager y actualice manualmente los recursos de Systems Manager creados 34
CloudFormation Utilícelo en lugar de Quick Setup 35
Configuración rápida personalizada en una sola cuenta y región con una CloudFormation pila 36
Configuración rápida personalizada en varias regiones y cuentas con CloudFormation StackSets 37
Consideraciones para configurar los servidores locales 39
Consideraciones sobre las instancias EC2 efímeras 40

Uso de una solución automatizada para implementar el agente CloudWatch 41
Despliegue del CloudWatch agente durante el aprovisionamiento de la instancia con el script de datos de usuario 41
Incluir el CloudWatch agente en su AMIs 42
Registro y supervisión en Amazon ECS 44
Configuración CloudWatch con un tipo de lanzamiento de EC2 44
Registros de contenedores de Amazon ECS para los tipos de lanzamiento de EC2 y Fargate ... 46
Uso del enrutamiento de registros personalizado con FireLens Amazon ECS 47
Métricas de Amazon ECS 48
Creación de métricas de aplicaciones personalizadas en Amazon ECS 49
Registro y monitoreo en Amazon EKS 51
Registro para Amazon EKS 51
Registro de plano de control de Amazon EKS 52
Registro de nodos y aplicaciones de Amazon EKS 52
Cómo iniciar sesión en Amazon EKS en Fargate 55
Métricas de Amazon EKS y Kubernetes 55
Métricas del plano de control de Kubernetes 56
Métricas de nodos y sistemas para Kubernetes 56
Métricas de aplicación 57
Métricas de Amazon EKS en Fargate 58
Supervisión de Prometheus en Amazon EKS 59
Registro y métricas para AWS Lambda 61
Registro de funciones Lambda 61
Envío de registros a otros destinos desde CloudWatch 62
Métricas de función de Lambda 63
Métricas a nivel de sistema 63
Métricas de aplicación 64
Búsqueda y análisis de los registros CloudWatch 65
Supervise y analice las aplicaciones de forma colectiva con Application Insights CloudWatch 65
Realizar análisis de CloudWatch registros con Logs Insights 68
Realizar análisis de registros con Amazon OpenSearch Service 70
Opciones alarmantes con CloudWatch 73
Uso de CloudWatch alarmas para monitorizar y emitir alarmas 73
Uso de la detección de CloudWatch anomalías para monitorear y emitir alarmas 74
Alarmante en varias regiones y cuentas 75
Automatizar la creación de alarmas con etiquetas de instancias EC2 75

Supervisión de la disponibilidad de aplicaciones y servicios 77
Rastreo de aplicaciones con AWS X-Ray 79
Implementación del daemon X-Ray para rastrear aplicaciones y servicios en Amazon EC2 80
Implementación del daemon X-Ray para rastrear aplicaciones y servicios en Amazon ECS o Amazon EKS 80
Configuración de Lambda para rastrear las solicitudes a X-Ray 81
Instrumentación de sus aplicaciones para X-Ray 81
Configuración de las reglas de muestreo de X-Ray 81
Cuadros de mando y visualizaciones con CloudWatch 83
Crear paneles de control multiservicio 83
Creación de cuadros de mando específicos para aplicaciones o cargas de trabajo 84
Crear paneles de control multicuentas o entre regiones 84
Usa la matemática métrica para afinar la observabilidad y las alarmas 85
Uso de paneles automáticos para Amazon ECS, Amazon EKS y Lambda CloudWatchContainer con Insights y Lambda Insights CloudWatch 86
CloudWatch integración con AWS servicios 87
Amazon Managed Grafana para la creación de paneles y la visualización 88
Preguntas frecuentes 92
¿Dónde guardo mis archivos CloudWatch de configuración? 92
¿Cómo puedo crear un ticket en mi solución de gestión de servicios cuando se produce una alarma? 92
¿Cómo puedo CloudWatch capturar los archivos de registro en mis contenedores? 92
¿Cómo superviso los problemas de salud de los AWS servicios? 93
¿Cómo puedo crear una CloudWatch métrica personalizada cuando no hay soporte de agentes? 93
¿Cómo puedo integrar mis herramientas de registro y supervisión existentes? AWS 93
Recursos 94
Introducción 94
Resultados empresariales específicos 94
Planificar su CloudWatch despliegue 94
Configuración del CloudWatch agente para las instancias EC2 y los servidores locales 94
CloudWatch enfoques de instalación de agentes para Amazon EC2 y servidores locales 95
Registro y supervisión en Amazon ECS 95
Registro y monitoreo en Amazon EKS 96
Registro y métricas para AWS Lambda 96
Búsqueda y análisis de los registros CloudWatch 97

Opciones alarmantes con CloudWatch 98
Supervisión de la disponibilidad de las aplicaciones y los servicios 98
Rastreo de aplicaciones con AWS X-Ray 98
Cuadros de mando y visualizaciones con CloudWatch 98
CloudWatch integración con AWS los servicios 98
Amazon Managed Grafana para la creación de paneles y la visualización 99
Historial de documentos 100
Glosario 101
..... 101
A 102
B 105
C 107
D 110
E 115
F 117
G 119
H 120
I 121
L 124
M 125
O 130
P 132
Q 135
R 136
S 139
T 143
U 144
V 145
W 145
Z 147
..... cxlviii

Diseño e implementación del registro y la supervisión con Amazon CloudWatch

Khurram Nizami, Amazon Web Services (AWS)

abril de 2023 (historial de documentos)

Esta guía le ayuda a diseñar e implementar el registro y la supervisión con Amazon CloudWatch y los servicios relacionados de administración y gobierno 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, DevOps ingenieros e ingenieros de aplicaciones que gestionan cargas de trabajo en la nube. AWS

Su enfoque de registro y monitoreo debe basarse en los seis pilares del AWS Well-Architected Framework. Estos pilares son la excelencia operativa, la seguridad, la confiabilidad, la eficiencia del rendimiento y la optimización de costos. Una solución de monitoreo y alarmas 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 supervisión para garantizar la seguridad o la optimización de los costes, ya que se trata de temas que requieren una evaluación exhaustiva. Hay muchos AWS servicios que admiten el registro y el monitoreo de seguridad AWS CloudTrail, AWS Configincluidos Amazon Inspector, Amazon Detective, Amazon Macie GuardDuty, Amazon y. AWS Security Hub CSPM También puede usar AWS Cost ExplorerAWS Budgets, y métricas de CloudWatch facturación para optimizar los costos.

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

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

Monitorización de métricas y alarmas	Identifique las observaciones y tendencias de sus cargas de trabajo y actúe en consecuencia.
Supervisión de la disponibilidad de las aplicaciones y los servicios	Reduzca el tiempo de inactividad y mejore su capacidad para cumplir los objetivos de nivel de servicio mediante la supervisión continua de la disponibilidad del servicio.
Aplicaciones de rastreo	Rastrea las solicitudes de las aplicaciones en los sistemas y las dependencias externas para ajustar el rendimiento, realizar análisis de 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 contribuye a la mejora continua y a la detección proactiva de los problemas.

CloudWatch puede cumplir con la mayoría de los requisitos de registro y supervisión y proporciona una solución fiable, escalable y flexible. Muchos AWS servicios proporcionan CloudWatch métricas automáticamente, además de la integración de CloudWatch registros para la supervisión 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 e informática sin servidores. Esta guía también incluye los siguientes AWS servicios que se utilizan con el registro y la supervisión:

- AWS Systems Manager Distributor, Systems Manager State Manager y Systems Manager Automation para automatizar, configurar y actualizar el CloudWatch agente para sus instancias EC2 y servidores locales
- Amazon OpenSearch Service para agregación, búsqueda y análisis avanzados de registros
- Amazon Route 53 realiza controles de estado y CloudWatchSynthetics para supervisar la disponibilidad de las aplicaciones y los servicios
- Amazon Managed Service para Prometheus para monitorizar aplicaciones en contenedores 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 varias fuentes (por ejemplo, CloudWatch Amazon OpenSearch Service y Amazon Timestream)

Los servicios de AWS cómputo que elija también afectan a la implementación y configuración de su 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 las aplicaciones y las cargas de trabajo suelen olvidarse del registro y la supervisión o configurarlos e implementarlos de forma incoherente. Esto significa que las cargas de trabajo entran en producción con una observabilidad limitada, lo que provoca demoras en la identificación de los problemas y aumenta el tiempo necesario para solucionarlos y resolverlos. Como mínimo, su solución de registro y supervisión debe abordar la capa de sistemas para los registros y las métricas a nivel del sistema operativo (SO), además de la capa de aplicación para los registros y las 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 EC2 inmutables y de larga duración	Registros y métricas de sistemas y aplicaciones en varios sistemas operativos (OSs) en varias AWS regiones o cuentas.
Contenedores	Registros y métricas del sistema y de la aplicación para sus clústeres de Amazon ECS y Amazon EKS, incluidos ejemplos de distintas configuraciones.
Sin servidor	Registros y métricas del sistema y de las aplicaciones para las funciones de Lambda y consideraciones para la personalización.

Esta guía proporciona una solución de registro y supervisión que aborda CloudWatch AWS los servicios relacionados en las siguientes áreas:

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

- Configuración del CloudWatch agente para las instancias EC2 y los servidores locales— detalles CloudWatch de configuración para los registros y las métricas a nivel del sistema y de la aplicación.
- CloudWatch enfoques de instalación de agentes para Amazon EC2 y servidores locales— Métodos para instalar el CloudWatch agente, incluida la implementación automática mediante Systems Manager en varias regiones y cuentas.
- Registro y supervisión en Amazon ECS— Guía CloudWatch para configurar los registros y las métricas a nivel de clúster y aplicación en Amazon ECS.
- Registro y monitoreo en Amazon EKS— Guía CloudWatch para configurar los registros y las métricas a nivel de clúster y aplicación en Amazon EKS.
- Supervisión de Prometheus en Amazon EKS— Presenta y compara Amazon Managed Service para Prometheus CloudWatch con la supervisión de Container Insights para Prometheus.
- Registro y métricas para AWS Lambda— Guía CloudWatch para configurar las funciones de Lambda.
- Búsqueda y análisis de los registros CloudWatch— Métodos para analizar sus registros mediante Amazon CloudWatch Application Insights y CloudWatch Logs Insights y para extender el análisis de registros a Amazon OpenSearch Service.
- Opciones alarmantes con CloudWatch— Introduce CloudWatch las alarmas y la detección de CloudWatch anomalías y proporciona orientación sobre la creación y configuración de las alarmas.
- Supervisión de la disponibilidad de aplicaciones y servicios— Introduce y compara las comprobaciones de estado de CloudWatch Synthetics y Route 53 para la supervisión automática de la disponibilidad.
- Rastreo de aplicaciones con AWS X-Ray— Introducción y configuración del rastreo de aplicaciones mediante X-Ray para Amazon EC2, Amazon ECS, Amazon EKS y Lambda
- Cuadros de mando y visualizaciones con CloudWatch— Introducción a los CloudWatch paneles de control para mejorar la observabilidad en todas las cargas de trabajo. AWS
- CloudWatch integración con AWS servicios— Explica cómo CloudWatch se integra con varios servicios. AWS
- Amazon Managed Grafana para la creación de paneles y la visualización— Presenta y compara Amazon Managed Grafana con los paneles y CloudWatch la visualización.

A lo largo de esta guía se utilizan ejemplos de implementación en estas áreas y también están disponibles en el repositorio de AWS muestras GitHub .

Resultados empresariales específicos

Crear una solución de registro y monitoreo diseñada para la AWS nube es fundamental para lograr las seis ventajas de la computación en 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 siguientes cuatro resultados después de implementar una solución de registro y monitoreo alineada con el AWS Well-Architected Framework:

Acelere la preparación operativa

Habilitar una solución de registro y monitoreo es un componente importante a la hora de preparar una carga de trabajo para el soporte y el uso de la producción. La preparación operativa puede convertirse rápidamente en un obstáculo si se depende demasiado de los procesos manuales y, además, puede reducir el tiempo de amortización (TTV) de sus inversiones en TI. Un enfoque ineficaz también reduce la observabilidad de las cargas de trabajo. Esto puede aumentar el riesgo de interrupciones prolongadas, insatisfacción de los clientes y procesos empresariales fallidos.

Puede utilizar los enfoques de esta guía para estandarizar y automatizar el registro y la supervisión en la nube. AWS Por lo tanto, 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 monitoreo a escala para diferentes cargas de trabajo en varias cuentas y regiones.

Mejore la excelencia operativa

Esta guía proporciona varias prácticas recomendadas para el registro y la supervisión que ayudan a las diversas cargas de trabajo a cumplir los objetivos empresariales y la excelencia operativa. Esta guía también proporciona ejemplos detallados y plantillas reutilizables de código abierto que puede utilizar con un enfoque de infraestructura como código (IaC) para implementar una solución de registro y supervisión bien diseñada mediante servicios. AWS Mejorar la excelencia operativa es iterativo y requiere una mejora continua. La guía proporciona sugerencias sobre cómo mejorar continuamente las prácticas de registro y monitoreo.

Mejore la visibilidad operativa

Sus procesos y aplicaciones empresariales pueden estar respaldados por diferentes recursos de TI y estar alojados en diferentes tipos de cómputo, ya sea de forma local o en la AWS nube. La visibilidad operativa puede verse limitada por las implementaciones inconsistentes 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 en todas sus cargas de trabajo. Esta guía le ayuda a diseñar e implementar enfoques para mejorar la visibilidad operativa completa y reducir el tiempo medio de resolución de los fallos (MTTR). Un enfoque integral de registro y monitoreo 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 (). SLAs

Amplíe las operaciones y reduzca los gastos generales

Puede escalar las prácticas de registro y monitoreo de esta guía para que sean compatibles con varias regiones y cuentas, recursos de corta duración y múltiples entornos. La guía proporciona enfoques y ejemplos para automatizar los pasos manuales (por ejemplo, instalar y configurar agentes, monitorear las métricas y notificar o tomar medidas cuando se producen problemas). Estos enfoques son útiles cuando la adopción de la nube madura y crece y si 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 cómputo y los OSs 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.

Recomendamos usarlo CloudWatch para capturar e ingerir registros y métricas para varios OSs 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 OSs 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 entre cuentas 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 tienen un equipo de operaciones y seguridad centralizado o 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 su arquitectura de 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 AWS SDK para crear 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 o a 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 individualmente. 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	Guarde los archivos de CloudWatch configuración estándar específicos de Windows para los servidores locales. 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.
/2 config/standard/linux/ec	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 CloudWatch los servidores locales. 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) 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 de sus cuentas y. Regiones de AWS

Configuración del CloudWatch agente para las instancias EC2 y los servidores locales

Muchas organizaciones ejecutan cargas de trabajo tanto en servidores físicos como en máquinas virtuales (). VMs Por lo general, estas cargas de trabajo se ejecutan en diferentes OSs plataformas y cada una tiene requisitos de instalación y configuración únicos para capturar e ingerir métricas.

Si opta por 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 para el registro y la supervisión, y aplicando un enfoque de instalación y configuración estándar para capturar e ingerir registros y métricas.

Organizations que migren o extiendan sus inversiones en TI a la AWS nube pueden aprovechar CloudWatch para lograr una solución unificada de registro y monitoreo. CloudWatch La fijación de precios significa que usted paga de forma incremental por las métricas y los registros que desee capturar. También puede capturar registros y métricas para servidores locales mediante un proceso de instalación de CloudWatch agentes similar al de Amazon EC2.

Antes de comenzar con la instalación y la implementación 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 OSs que desee utilizar. Los registros y las métricas del sistema son la base y el estándar de una solución de registro y supervisión porque los genera 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 los que son específicos de una versión o distribución de Linux. Esta variación también se produce entre las distintas versiones de Windows.

Configuración del agente CloudWatch

CloudWatch captura métricas y registros para Amazon EC2 y los servidores locales mediante CloudWatch agentes y archivos de configuración de agentes 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 empezar a instalar el CloudWatch agente a escala en sus cuentas.

Puede combinar varias configuraciones de CloudWatch agentes para formar una configuración de CloudWatch agente compuesta. Un enfoque recomendado consiste en definir y dividir las

configuraciones de los registros y las métricas a nivel del sistema y de la aplicación. El siguiente diagrama ilustra cómo se pueden combinar varios tipos de archivos de CloudWatch configuración para diferentes requisitos para formar una CloudWatch configuración compuesta:

Estos registros y métricas también se pueden clasificar y configurar aún más para entornos o requisitos específicos. Por ejemplo, puede 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 los archivos de registro. En su lugar, el software del CloudWatch agente instalado en la instancia, la AWS API o AWS Command Line Interface () de EC2 captura los archivos de registro y los ingiere en los CloudWatch registros.AWS CLI Recomendamos utilizar el CloudWatch agente para introducir archivos de registro en CloudWatch Logs for Amazon EC2 y en servidores locales.

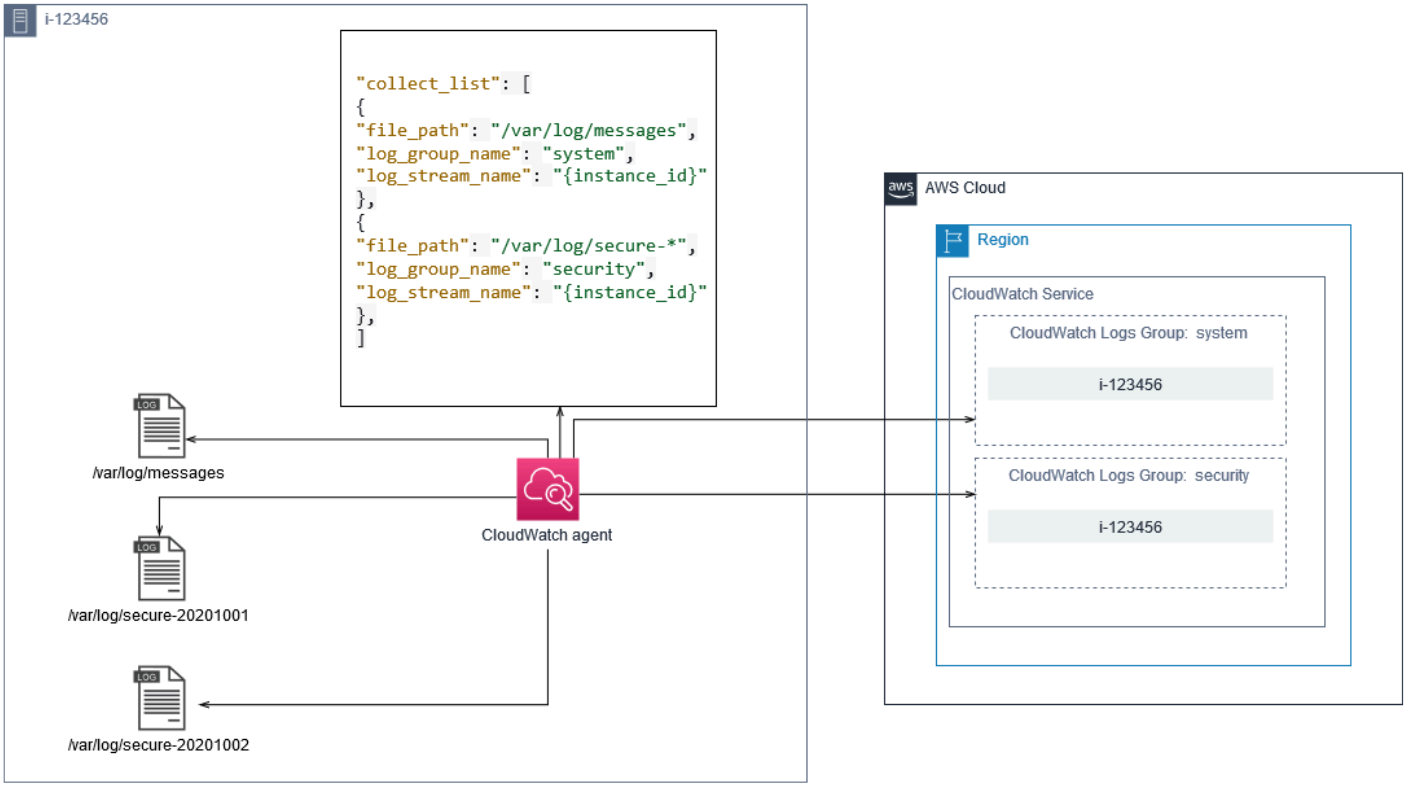
Puede buscar y filtrar los registros, así como extraer métricas y ejecutar la automatización en función de los patrones de aplicación de parches a partir de los archivos de registro incluidos. CloudWatch CloudWatch admite opciones de sintaxis de filtros y patrones de texto sin formato, delimitados por espacios y con formato JSON, mientras que los registros con formato JSON ofrecen la mayor flexibilidad. Para aumentar las opciones de filtrado y análisis, debe utilizar una salida de registro formateada en lugar de texto sin formato.

El CloudWatch agente utiliza un archivo de configuración que define los registros y las métricas a los que se va a CloudWatch enviar. CloudWatch a continuación, captura cada archivo de registro como un flujo de registro y agrupa estos flujos de registro en un grupo de registros. Esto le ayuda a realizar operaciones en los registros de sus instancias de EC2, como buscar una cadena coincidente.

El nombre del flujo de registro predeterminado es el mismo que el ID de la instancia 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 en el grupo de CloudWatch registros. Puede utilizar`instance_id`, `hostnamelocal_hostname`, o `ip_address` para la sustitución dinámica en los nombres del flujo de registro y de los grupos de registros, lo que significa que puede utilizar el mismo archivo de configuración del CloudWatch agente en varias instancias de EC2.

El siguiente diagrama muestra la configuración de un CloudWatch 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, ya que la `{instance_id}` variable se utiliza para el nombre del flujo de registro y la instancia IDs de EC2 es única.



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 agrupamiento predeterminado basado en el nombre del archivo de registro permite buscar, crear métricas y generar alarmas sobre los datos específicos de un archivo de registro en todas las instancias de EC2 de una cuenta y una región. Debe evaluar si es necesario refinar más los grupos de registros. Por ejemplo, es posible que su cuenta la compartan varias unidades de negocio y que tengan distintos propietarios técnicos o de operaciones. Esto significa que debe refinar aún más el nombre del grupo de registros para que refleje la separación y la propiedad. Este enfoque le permite concentrar el análisis y la solución de problemas en la instancia de EC2 correspondiente.

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

Nombre del grupo de registro	`/<Business unit>/<Project or application name>/<Environment>/<Log file name>`
Nombre del flujo de registro	`<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 para una sola instancia de EC2. Esto resulta útil si la mayoría de las instancias de EC2 dan servicio a una aplicación o carga de trabajo y cada instancia de EC2 tiene un propósito específico. En la siguiente tabla se muestra cómo se puede formatear la denominación de sus grupos de registros y flujos de registros para respaldar este enfoque.

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

Configuración de la captura de métricas para instancias EC2

De forma predeterminada, las instancias EC2 están habilitadas para la supervisión básica y se envía automáticamente un conjunto estándar de métricas (por ejemplo, métricas relacionadas con la CPU, la red o el almacenamiento) cada cinco minutos. CloudWatch CloudWatch las métricas pueden variar en función de la familia de instancias; por ejemplo, las instancias de rendimiento en ráfagas tienen métricas para los créditos de CPU. Las métricas estándar de Amazon EC2 están incluidas en el precio de la instancia. Si habilita la supervisión detallada de sus instancias EC2, podrá recibir datos en períodos de un minuto. La frecuencia de los períodos afecta a sus CloudWatch costos, así que asegúrese de evaluar si se requiere una supervisión detallada para todas sus instancias de EC2 o solo para algunas de ellas. Por ejemplo, puede habilitar la supervisión detallada de las cargas de trabajo de producción, pero utilizar la supervisión básica para las cargas de trabajo que no son de producción.

Los servidores locales no incluyen ninguna métrica predeterminada CloudWatch y deben usar el CloudWatch agente o el AWS SDK para capturar AWS CLI las métricas. Esto significa que debe definir las métricas que desea capturar (por ejemplo, el uso de la CPU) en el archivo de CloudWatch configuración. Puede crear un archivo de CloudWatch configuración único que incluya las métricas de instancia EC2 estándar para los servidores locales y aplicarlo además de la configuración estándar CloudWatch .

Las métricas CloudWatch se definen de forma exclusiva mediante el nombre de la métrica y cero o más dimensiones, y se agrupan de forma única en un espacio de nombres de métricas. Las métricas proporcionadas por un AWS servicio tienen un espacio de nombres que comienza por `AWS` (por ejemplo,`AWS/EC2`) y las que no son AWS métricas se consideran métricas personalizadas. Todas las métricas que se configuran y capturan con el CloudWatch agente se consideran métricas personalizadas. Dado que la cantidad de métricas creadas afecta a sus CloudWatch costes, debe evaluar si cada métrica es necesaria para todas las instancias de EC2 o solo para algunas de ellas. Por ejemplo, puede definir un conjunto completo de métricas para las cargas de trabajo de producción, pero utilizar un subconjunto más pequeño de estas métricas para las cargas de trabajo que no son de producción.

`CWAgent`es el espacio de nombres predeterminado para las métricas publicadas por el agente. CloudWatch Al igual que 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 que refleje una unidad de negocio, un proyecto o una aplicación y un 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 la convención de nomenclatura de los grupos de CloudWatch registros.

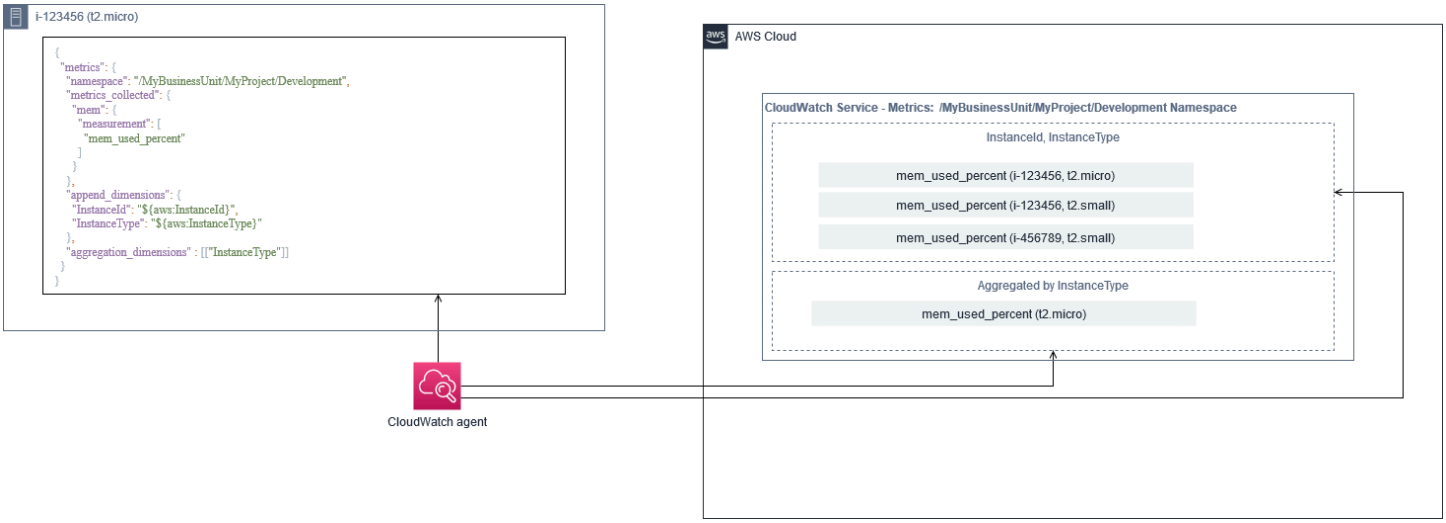
Las métricas también se identifican por sus dimensiones, que ayudan a analizarlas en función de un conjunto de condiciones, y son las propiedades con las que se registran las observaciones. Amazon EC2 incluye métricas independientes para las instancias EC2 con `InstanceId` dimensiones y dimensiones. `AutoScalingGroupName` También recibirá métricas con las `InstanceType` dimensiones `ImageId` y si habilita la supervisión detallada. Por ejemplo, Amazon EC2 proporciona una métrica de instancia EC2 independiente para el uso de la CPU con las `InstanceId` dimensiones, además de una métrica de uso de la CPU independiente para la dimensión. `InstanceType` Esto le ayuda a analizar el uso de la CPU para cada instancia EC2 única, además de todas las instancias EC2 de un tipo de instancia específico.

Agregar más dimensiones aumenta la capacidad de análisis, pero también aumenta los costos generales, ya que cada combinación de métrica y valor de dimensión único da como resultado una nueva métrica. Por ejemplo, si crea una métrica para el porcentaje de uso de memoria en relación con la `InstanceId` dimensión, se trata de una métrica nueva para cada instancia de EC2. Si su organización ejecuta miles de instancias EC2, esto genera miles de métricas y se traduce en costes más altos. Para controlar y predecir los costos, asegúrese de determinar la cardinalidad de la métrica y qué dimensiones añaden más valor. Por ejemplo, puede definir un conjunto completo de dimensiones para las métricas de la carga de trabajo de producción, pero un subconjunto más pequeño de estas dimensiones para las cargas de trabajo ajenas a la producción.

Puede usar la `append_dimensions` propiedad para agregar dimensiones a una o todas las métricas definidas en su configuración. CloudWatch También puede añadir dinámicamente las métricas`ImageId`, `InstanceIdInstanceType`, y `AutoScalingGroupName` a todas las métricas de la CloudWatch configuración. Como alternativa, puede agregar un nombre y un valor de dimensión arbitrarios para métricas específicas mediante la `append_dimensions` propiedad de esa métrica. CloudWatch también puede agregar estadísticas sobre las dimensiones métricas que haya definido con la `aggregation_dimensions` propiedad.

Por ejemplo, puede sumar la memoria utilizada con respecto a la `InstanceType` dimensión para ver la memoria promedio utilizada por todas las instancias de EC2 para cada tipo de instancia. Si usa `t2.micro` instancias que se ejecutan en una región, puede determinar si las cargas de trabajo que utilizan la `t2.micro` clase están sobreutilizando o infrautilizando la memoria proporcionada. La infrautilización puede ser una señal de que las cargas de trabajo utilizan clases de EC2 con una capacidad de memoria no requerida. Por el contrario, la sobreutilización puede ser una señal de que las cargas de trabajo utilizan clases de Amazon EC2 con memoria insuficiente.

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



Configuración a nivel de sistema CloudWatch

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

Le recomendamos que utilice el asistente de archivos de CloudWatch configuración o el esquema de archivos de configuración para definir el archivo de configuración del CloudWatch agente para cada sistema operativo que vaya a admitir. Se pueden definir registros y métricas adicionales específicos de la carga de trabajo a nivel del sistema operativo en archivos de CloudWatch configuración independientes y añadirlos a la configuración estándar. Estos archivos de configuración únicos deben almacenarse por separado en un depósito de S3 donde las instancias de EC2 puedan recuperarlos. En la Administrar CloudWatch las configuraciones sección de esta guía se describe un ejemplo de configuración de un bucket de S3 para este propósito. Puede recuperar y aplicar estas configuraciones automáticamente mediante State Manager y Distributor.

Configuración de registros a nivel de sistema

Los registros a nivel del sistema son esenciales para diagnosticar y solucionar problemas en las instalaciones o en la nube. AWS Su enfoque de captura de registros debe incluir todos los registros del sistema y de seguridad generados por el sistema operativo. Los archivos de registro generados por el sistema operativo pueden ser diferentes según la versión del sistema operativo.

El CloudWatch agente permite supervisar 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 `SystemApplication`, o`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 más comunes que debe supervisar, pero debe comprobar el `/etc/syslog.conf` archivo `/etc/rsyslog.conf` o para determinar la configuración específica de los archivos de registro del sistema.

Distribución de Fedora (Amazon Linux, Centos, Red Hat Enterprise Linux)	`/var/log/boot.log*` — Registro de arranque
	`/var/log/dmesg` — Registro del núcleo
	`/var/log/secure` — Registro de seguridad y autenticación
	`/var/log/messages` — Registro general del sistema
	`/var/log/cron*` — Registros de Cron
	`/var/log/cloud-init-output.log` — Salida de los scripts de `Userdata` inicio
Debian (Ubuntu)	`/var/log/syslog` — Registro de arranque
	`/var/log/cloud-init-output.log` — Salida de los scripts de `Userdata` inicio
	`/var/log/auth.log` — Registro de seguridad y autenticación
	`/var/log/kern.log` — Registro del núcleo

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

Windows	CloudWatch agente	`$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	CloudWatch agente	`/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 está definido en la configuración del CloudWatch agente, pero no se encuentra. Esto resulta útil cuando se quiere mantener una configuración de registro única para Linux, en lugar de configuraciones independientes para cada

distribución. También resulta útil cuando un archivo de registro no existe hasta que el agente o la aplicación de software comiencen a ejecutarse.

Configurar métricas a nivel de sistema

La utilización de memoria y espacio en disco no se incluye en las métricas estándar que proporciona Amazon EC2. Para incluir estas métricas, debe instalar y configurar el CloudWatch agente en las instancias de EC2. El asistente de configuración del CloudWatch agente crea una CloudWatch configuración con métricas predefinidas y usted 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 la carga de trabajo deben publicar métricas del sistema adicionales en función de los requisitos específicos de un servidor o una instancia de EC2. Estas definiciones de métricas deben almacenarse, versionarse y mantenerse en un archivo de configuración de CloudWatch agente independiente y compartirse 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 archivo de configuración del CloudWatch agente utilizado por las instancias locales. Puede crear un archivo de configuración de métricas independiente para las instancias locales con métricas como el uso de la CPU y adjuntar estas métricas al archivo de configuración de métricas estándar.

Configuración a nivel de aplicación CloudWatch

Los registros y las métricas de las aplicaciones se generan al ejecutar las aplicaciones y son específicos de cada aplicación. Asegúrese de definir los registros y las métricas necesarios para supervisar adecuadamente las aplicaciones que su organización utiliza habitualmente. Por ejemplo, es posible que su organización haya estandarizado el Microsoft Internet Information Server (IIS) para las aplicaciones basadas en la web. Puede crear una CloudWatch configuración de registro y métrica estándar para IIS que también se pueda 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 pueden acceder a ellos o mediante una recuperación automática y copiarlos en el CloudWatch directorio de configuración. El CloudWatch agente combina automáticamente los archivos de CloudWatch configuración que se encuentran en el directorio de archivos de configuración de cada instancia o servidor EC2 en una configuración compuesta. CloudWatch El resultado final es una CloudWatch configuración

que incluye la configuración estándar a nivel de sistema de su organización, así como todas las configuraciones relevantes a nivel de aplicación. CloudWatch

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

Configurar los registros a nivel de aplicación

El registro a nivel de aplicación varía en función de si se trata de una aplicación comercial off-the-shelf (COTS) o desarrollada a medida. Las aplicaciones COTS y sus componentes pueden ofrecer varias opciones para la configuración y la salida del registro, como el nivel de detalle del registro, el formato del archivo de registro y la ubicación del archivo de registro. Sin embargo, la mayoría de las aplicaciones COTS o de terceros no permiten cambiar el registro de manera fundamental (por ejemplo, actualizar el código de la aplicación para incluir instrucciones de registro adicionales o formatos que no son configurables). Como mínimo, debe configurar las opciones de registro para que los COTS o las aplicaciones de terceros registren la información de advertencia y nivel de error, preferiblemente en formato JSON.

Puede integrar aplicaciones desarrolladas a medida con CloudWatch Logs incluyendo los archivos de registro de la aplicación en su configuración. CloudWatch Las aplicaciones personalizadas proporcionan una mejor calidad y control del registro, ya que puede personalizar el formato de salida del registro, categorizar y separar la salida de los componentes en archivos de registro independientes, además de incluir cualquier detalle adicional necesario. Asegúrese de revisar y estandarizar las bibliotecas de registro, así como los datos y el formato necesarios para su organización, a fin de facilitar el análisis y el procesamiento.

También puede escribir en un flujo de CloudWatch registro con la llamada a la `PutLogEvents` API CloudWatch Logs o mediante el AWS SDK. Puedes usar la API o el SDK para cumplir con los 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 consiste en configurar las aplicaciones para que escriban en los archivos de registro y, a continuación, utilizar el CloudWatch agente para leer y transmitir los archivos de registro CloudWatch.

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

También puede crear métricas personalizadas para las aplicaciones desarrolladas a medida mediante el formato de métricas CloudWatch integrado en los archivos de registro de las aplicaciones.

Configuración de métricas a nivel de aplicación

Las métricas personalizadas son métricas que los AWS servicios no proporcionan directamente CloudWatch y que se publican en un espacio de nombres personalizado en las métricas. CloudWatch Todas las métricas de la aplicación se consideran métricas personalizadas CloudWatch . Las métricas de la aplicación pueden alinearse con una instancia de EC2, un componente de la aplicación, una llamada a la API o incluso una función empresarial. También debe tener en cuenta la importancia y la cardinalidad de las dimensiones que elija para sus métricas. Las dimensiones con una cardinalidad alta generan una gran cantidad de métricas personalizadas y podrían aumentar sus CloudWatch costes.

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

- Capture las métricas a nivel de proceso definiendo los procesos individuales que desea capturar desde el complemento procstat.
- Una aplicación publica una métrica en el Monitor de rendimiento de Windows y esta métrica se define en la configuración. CloudWatch
- Los filtros y patrones métricos se aplican a los inicios de sesión de una aplicación CloudWatch.
- Una aplicación escribe en un CloudWatch registro mediante el formato métrico CloudWatch incorporado.
- Una aplicación envía una métrica a CloudWatch través de la API o el AWS SDK.
- Una aplicación envía una métrica a un daemon de Collectd o StatsD con un agente configurado. CloudWatch

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

La supervisión de Procstat también es útil si no puede actualizar sus aplicaciones COTS con métricas personalizadas adicionales. Por ejemplo, puede crear una `my_process` métrica que mida

`cpu_time` e incluya una `application_version` dimensión personalizada. También puede usar varios archivos de configuración de CloudWatch agentes para una aplicación si tiene dimensiones diferentes para métricas diferentes.

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

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

En el caso de las aplicaciones desarrolladas a medida, trabaje con los desarrolladores de la aplicación para definir las métricas importantes que se puedan implementar mediante el formato de métricas CloudWatch integrado, el AWS SDK o AWS la API. El enfoque recomendado consiste en utilizar el formato métrico integrado. Puede utilizar las bibliotecas de formato métrico integradas de código abierto que se AWS proporcionan para ayudarle a escribir sus declaraciones en el formato requerido. También tendría que actualizar la CloudWatch configuración específica de la aplicación para incluir el agente de formato métrico integrado. Esto hace que el agente que se ejecuta en la instancia EC2 actúe como un punto final local con formato métrico integrado al que envía las métricas con formato métrico integrado. CloudWatch

Si sus aplicaciones ya admiten la publicación de métricas en collectd o statsd, puede aprovecharlas para incorporarlas. CloudWatch

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

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

- Instalación del CloudWatch agente mediante Systems Manager Distributor y Systems Manager State Manager: se recomienda utilizar este enfoque si las instancias de EC2 y los servidores locales ejecutan el agente de Systems Manager. Esto garantiza que el CloudWatch agente se mantenga actualizado y que pueda informar sobre los servidores que no tienen el agente y corregirlos. CloudWatch 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 al arrancar o reiniciar por primera vez. Puede definir un script para automatizar el proceso de descarga e instalación del agente. Esto también se puede incluir en los CloudFormation scripts y en los productos AWS de Service Catalog. Este enfoque puede ser adecuado según sea necesario si existe un enfoque personalizado de instalación y configuración de agentes para una carga de trabajo específica que se desvíe de sus estándares.
- Incluir el CloudWatch agente en Amazon Machine Images (AMIs): puede instalar el CloudWatch agente en sus AMI personalizadas para Amazon EC2. Las instancias EC2 que utilizan la AMI instalarán e iniciarán automáticamente el agente. Sin embargo, debe asegurarse de que el agente y su configuración se actualicen periódicamente.

Instalación del CloudWatch agente mediante Systems Manager Distributor y State Manager

Puede usar Systems Manager State Manager con Systems Manager Distributor para instalar y actualizar automáticamente el CloudWatch agente en los servidores y las instancias de EC2. El distribuidor incluye el paquete `AmazonCloudWatchAgent` AWS gestionado que instala la versión más reciente del CloudWatch agente.

Este enfoque de instalación tiene los siguientes requisitos previos:

- El agente de Systems Manager debe estar instalado y en ejecución en sus servidores o instancias EC2. El agente Systems Manager viene preinstalado en Amazon Linux y Amazon Linux 2, entre otros AMIs. El agente también debe estar instalado y configurado en otras imágenes o en servidores VMs y locales.

  > **Note**
  >
  > Se acerca el fin de la compatibilidad de Amazon Linux 2. Para obtener más información, consulte Amazon Linux 2 FAQs.

- Un rol o credenciales de IAM que tengan los permisos necesarios CloudWatch y de Systems Manager deben adjuntarse a la instancia EC2 o definirse en el archivo de credenciales de un servidor local. Por ejemplo, puede crear un rol de IAM que incluya las políticas AWS administradas: `AmazonSSMManagedInstanceCore` para Systems Manager y `CloudWatchAgentServerPolicy` para CloudWatch. Puedes usar la CloudFormation plantilla ssm-cloudwatch-instance-role.yaml para implementar un rol de IAM y un perfil de instancia que incluyan estas dos políticas. Esta plantilla también se puede modificar para incluir otros permisos de IAM estándar para las instancias de EC2. Para servidores locales o VMs, debe configurar el CloudWatch agente para que utilice la función de servicio Systems Manager que se configuró para el servidor local. Para obtener más información al respecto, consulte ¿Cómo puedo configurar los servidores locales que utilizan el Agente de Systems Manager y el CloudWatch agente unificado para que usen solo credenciales temporales? en el Centro de AWS conocimiento.

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

- Instalación automática para varios sistemas OSs: no es necesario escribir ni mantener un script para cada sistema operativo para descargar e instalar el CloudWatch agente.
- Comprobaciones de actualización automáticas: State Manager comprueba de forma automática y periódica que cada instancia de EC2 tenga la CloudWatch versión más reciente.
- Informes de conformidad: el panel de conformidad de Systems Manager muestra qué instancias de EC2 no pudieron instalar correctamente el paquete Distributor.
- Instalación automática para las instancias de EC2 recién lanzadas: las nuevas instancias de EC2 que se lanzan a su cuenta reciben automáticamente el agente. CloudWatch

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, las dos asociaciones podrían interferir entre sí y provocar problemas. Al utilizar este enfoque, debe eliminar cualquier asociación existente que instale o actualice el CloudWatch agente y la configuración.
- Actualización de los archivos de configuración del agente personalizados: el distribuidor realiza una instalación mediante el archivo de configuración predeterminado. Si utiliza un archivo de configuración personalizado o varios archivos de CloudWatch configuración, debe actualizar la configuración después de la instalación.
- Configuración multirregional o multicuenta: la asociación de administradores estatales debe estar configurada en cada cuenta y región. Las cuentas nuevas en un entorno de múltiples cuentas deben actualizarse para incluir la asociación de administradores estatales. Debe centralizar o sincronizar la CloudWatch configuración para que varias cuentas y regiones puedan recuperar y aplicar los estándares requeridos.

Configure State Manager y Distributor para el despliegue y la configuración de los CloudWatch agentes

Puede utilizar Systems Manager Quick Setup para configurar rápidamente las funciones de Systems Manager, incluida la instalación y actualización automáticas del CloudWatch agente en las instancias EC2. La configuración rápida despliega una CloudFormation pila que despliega y configura los recursos de Systems Manager en función de sus elecciones.

La siguiente lista proporciona dos acciones importantes que realiza Quick Setup para la instalación y actualización automatizadas de los CloudWatch agentes:

1. Crear documentos personalizados de Systems Manager: Quick Setup crea los siguientes documentos de Systems Manager para usarlos con State Manager. Los nombres de los documentos pueden variar, pero el contenido sigue siendo el mismo:
   - `CreateAndAttachIAMToInstance`— Crea el `AmazonSSMRoleForInstancesQuickSetup` rol y el perfil de instancia si no existen y adjunta la `AmazonSSMManagedInstanceCore` política al rol. Esto no incluye la política de `CloudWatchAgentServerPolicy` IAM requerida. Debe actualizar esta política y este documento de Systems Manager para incluir esta política, tal como se describe en la siguiente sección.

- `InstallAndManageCloudWatchDocument`— Instala el CloudWatch agente con Distributor y configura cada instancia de EC2 una vez con una configuración de CloudWatch agente predeterminada mediante el documento `AWS-ConfigureAWSPackage` Systems Manager.
- `UpdateCloudWatchDocument`— Actualiza el CloudWatch agente instalando el CloudWatch agente más reciente mediante el documento `AWS-ConfigureAWSPackage` Systems Manager. Al actualizar o desinstalar el agente no se eliminan los archivos de CloudWatch configuración existentes de la instancia EC2.

2. Crear asociaciones de administradores de estados: las asociaciones de administradores de estados se crean y configuran para usar los documentos de Systems Manager creados a medida. Los nombres de las asociaciones de administradores estatales pueden variar, pero la configuración sigue siendo la misma:
   - `ManageCloudWatchAgent`— Ejecuta el documento `InstallAndManageCloudWatchDocument` Systems Manager una vez para cada instancia de EC2.
   - `UpdateCloudWatchAgent`— Ejecuta el documento de `UpdateCloudWatchDocument` Systems Manager cada 30 días para cada instancia de EC2.
   - Ejecuta el documento de `CreateAndAttachIAMToInstance` Systems Manager una vez para cada instancia de EC2.

Debe aumentar y personalizar la configuración de configuración rápida completa para incluir CloudWatch permisos y admitir configuraciones personalizadas CloudWatch . En particular, será necesario actualizar el `InstallAndManageCloudWatchDocument` documento `CreateAndAttachIAMToInstance` y el documento. Puede actualizar manualmente los documentos de Systems Manager creados por Quick Setup. Como alternativa, puede usar su propia CloudFormation plantilla para aprovisionar los mismos recursos con las actualizaciones necesarias, así como configurar e implementar otros recursos de Systems Manager y no usar Quick Setup.

> **Important**
>
> La configuración rápida crea una CloudFormation pila 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 Quick Setup, así como utilizar su propia CloudFormation plantilla para realizar una Quick Setup actualizada. Le recomendamos que utilice su propia CloudFormation plantilla para evitar actualizar manualmente los recursos creados por Quick Setup y CloudFormation.

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

Los recursos de Systems Manager creados por el enfoque de configuración rápida deben actualizarse para incluir los permisos de CloudWatch agente necesarios y admitir varios archivos de CloudWatch configuración. En esta sección se describe cómo actualizar la función de IAM y los documentos de Systems Manager para utilizar un bucket S3 centralizado que contenga CloudWatch configuraciones accesibles desde varias cuentas. En la Administrar CloudWatch las configuraciones sección de esta guía se describe la creación de un bucket de S3 para almacenar los archivos de CloudWatch configuración.

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

Este documento de Systems Manager creado por Quick Setup comprueba si una instancia EC2 tiene un perfil de instancia de IAM existente adjunto. Si lo tiene, adjunta la `AmazonSSMManagedInstanceCore` política al rol existente. Esto evita que las instancias EC2 existentes pierdan AWS los permisos que podrían asignarse a través de los perfiles de instancia existentes. Debe añadir un paso en este documento para adjuntar la política de `CloudWatchAgentServerPolicy` IAM a las instancias de EC2 que ya tienen un perfil de instancia adjunto. El documento Systems Manager también crea el rol de IAM si no existe y una instancia EC2 no tiene un perfil de instancia adjunto. Debe actualizar esta sección del documento para incluir también la política de `CloudWatchAgentServerPolicy` IAM.

Revise el documento de muestra CreateAndAttachIAMToInstance.yaml completo y compárelo con el documento creado por Quick Setup. Edite el documento existente para incluir los pasos y cambios necesarios. Según las opciones de configuración rápida, el documento creado por Quick Setup podría ser diferente del documento de muestra proporcionado, por lo que debe asegurarse de realizar los ajustes necesarios. El documento de muestra incluye la opción de configuración rápida para escanear las instancias a diario en busca de parches faltantes y, por lo tanto, incluye una política para el administrador de parches de Systems Manager.

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

Este documento de Systems Manager creado por Quick Setup instala el CloudWatch agente y lo configura con la configuración de CloudWatch agente predeterminada. La CloudWatch configuración predeterminada se alinea con el conjunto de métricas básico predefinido. Debe reemplazar el paso de configuración predeterminado y añadir pasos para descargar los archivos de CloudWatch configuración del bucket de CloudWatch configuración de S3.

Revise el documento actualizado con el InstallAndManageCloudWatchDocumentarchivo.yaml completo y compárelo con el documento creado por Quick Setup. El documento creado con la configuración rápida puede ser diferente, así que asegúrate de haber realizado los ajustes necesarios. Edite el documento existente para incluir los pasos y cambios necesarios.

CloudFormation Utilícelo en lugar de Quick Setup

En lugar de utilizar Quick Setup, puede CloudFormation utilizarla para configurar Systems Manager. Este enfoque le permite personalizar la configuración de Systems Manager de acuerdo con sus requisitos específicos. Este enfoque también evita las actualizaciones manuales de los recursos configurados de Systems Manager creados por Quick Setup para admitir CloudWatch configuraciones personalizadas.

La función de configuración rápida también utiliza CloudFormation y crea un conjunto de CloudFormation pilas para implementar y configurar los recursos de Systems Manager en función de sus elecciones. Antes de poder utilizar los conjuntos de CloudFormation pilas, debe crear las funciones de IAM que se utilizan CloudFormation StackSets para respaldar las implementaciones en varias cuentas o regiones. Quick Setup crea las funciones necesarias para respaldar las implementaciones en varias regiones o cuentas. CloudFormation StackSets Debe cumplir los requisitos previos CloudFormation StackSets si desea configurar e implementar los recursos de Systems Manager en varias regiones o en varias cuentas desde una sola cuenta y región. Para obtener más información al respecto, consulte los requisitos previos para las operaciones de conjuntos de pilas en la CloudFormation documentación.

Consulte la CloudFormation plantilla AWS- QuickSetup - SSMHost Mgmt.yaml para obtener una configuración rápida personalizada.

Debe revisar los recursos y las capacidades de la CloudFormation plantilla y hacer los ajustes necesarios según sus necesidades. Debe controlar las versiones de la CloudFormation plantilla que

utiliza y probar los cambios de forma incremental para confirmar el resultado requerido. Además, debe realizar revisiones de seguridad en la nube para determinar si es necesario realizar algún ajuste de política en función de los requisitos de su organización.

Debe implementar la CloudFormation pila en una sola cuenta de prueba y región, y realizar todos los casos de prueba necesarios para personalizar y confirmar el resultado deseado. A continuación, puede transferir el despliegue a varias regiones en una sola cuenta y, después, a varias cuentas y regiones.

Configuración rápida personalizada en una sola cuenta y región con una CloudFormation pila

Si solo usa una cuenta y una región, puede implementar el ejemplo completo como una CloudFormation pila en lugar de como un conjunto de CloudFormation pilas. Sin embargo, si es posible, te recomendamos que utilices el enfoque de conjuntos apilados con varias cuentas y regiones, aunque solo utilices una sola cuenta y región. Su uso CloudFormation StackSets facilita la expansión a cuentas y regiones adicionales en el futuro.

Siga los siguientes pasos para implementar la CloudFormation plantilla AWS- QuickSetup - SSMHost Mgmt.yaml como una CloudFormation pila en una sola cuenta y: Región de AWS

1. Descargue la plantilla y compruébela en su sistema de control de versiones preferido (por ejemplo,). GitHub
2. Personalice los valores de los CloudFormation parámetros predeterminados en función de los requisitos de su organización.
3. Personalice los horarios de la asociación de directores estatales.
4. Personalice el documento de Systems Manager con el identificador `InstallAndManageCloudWatchDocument` lógico. Confirme que los prefijos del bucket de S3 se alinean con los prefijos del bucket de S3 que contiene su CloudWatch configuración.
5. Recupere y registre el nombre de recurso de Amazon (ARN) del bucket de S3 que contiene sus CloudWatch configuraciones. Para obtener más información al respecto, consulte la Administrar CloudWatch las configuraciones sección de esta guía. Hay disponible un ejemplo de cloudwatch-config-splantilla.yaml de 3 CloudFormation compartimentos que incluye una política de compartimentos para proporcionar acceso de lectura a las cuentas. AWS Organizations
6. Implemente la CloudFormation plantilla de configuración rápida personalizada en la misma cuenta que su bucket de S3:

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

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

- Solicite la asociación de administradores `AttachIAMToInstance` estatales. Este es un manual de ejecución de Systems Manager que está configurado para ejecutarse según una programación. Las asociaciones de administradores de estados que utilizan manuales de ejecución 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, consulte Ejecución de automatizaciones con activadores mediante State Manager en la documentación de Systems Manager.
- Confirme que la instancia EC2 tenga asociada 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 consultando CloudWatch los registros y las métricas en función de las CloudWatch configuraciones del bucket de S3.

Configuración rápida personalizada en varias regiones y cuentas con CloudFormation StackSets

Si utiliza varias cuentas y regiones, puede implementar la CloudFormation plantilla AWS-QuickSetup - SSMHost Mgmt.YAML como un conjunto de pilas. Debe cumplir los CloudFormation StackSetrequisitos previos antes de usar los conjuntos de pilas. Los requisitos varían en función de si se despliegan conjuntos de pilas con permisos autogestionados o gestionados porservicios.

Le recomendamos que implemente conjuntos de pilas con permisos administrados por el servicio para que las nuevas cuentas reciban automáticamente la configuración rápida personalizada. Debe implementar un conjunto de pilas gestionado por el servicio desde la cuenta de AWS Organizations administración o la cuenta de administrador delegado. Debe implementar el conjunto de pilas desde una cuenta centralizada utilizada para la automatización y que tenga privilegios de administrador delegados, en lugar de desde la cuenta de administración. AWS Organizations También le recomendamos que pruebe la implementación de su conjunto de conjuntos apilados dirigiéndose a una unidad organizativa (OU) de prueba con un número único o reducido de cuentas en una región.

1. Complete los pasos 1 a 5 de la Configuración rápida personalizada en una sola cuenta y región con una CloudFormation pila sección de esta guía.
2. Inicie sesión en Consola de administración de AWS, abra la CloudFormation consola y seleccione Crear StackSet:
   - Selecciona La plantilla está lista y sube un archivo de plantilla. Cargue la CloudFormation plantilla que personalizó según sus necesidades.
   - Especifique los detalles del conjunto de pilas:
     - Introduzca el nombre de un conjunto de pilas, por ejemplo,`StackSet-SSM-QuickSetup`.
     - Realice ajustes en las opciones de los parámetros en función de las capacidades que desee habilitar para Systems Manager.
     - Para el `CloudWatchConfigBucketARN` parámetro, introduzca el ARN del bucket S3 de su CloudWatch configuración.
     - Especifique las opciones del conjunto de pilas y elija si va a utilizar los permisos gestionados por el servicio con permisos autogestionados AWS Organizations o los permisos autogestionados.
       - Si elige permisos autogestionados, introduzca los detalles de la función de IAM AWSCloudFormationStackSetAdministrationRoley los detalles de la función de IAM AWSCloudFormationStackSetExecutionRole. El rol de administrador debe existir en la cuenta y el rol de ejecución debe existir en cada cuenta de destino
     - Para los permisos administrados por el servicio con AWS Organizations, le recomendamos que primero los implemente en una unidad organizativa de prueba en lugar de en toda la organización.
       - Elija si desea habilitar las implementaciones automáticas. Le recomendamos que elija Activado. Para el comportamiento de eliminación de cuentas, la configuración recomendada es Eliminar pilas.
     - Para los permisos autogestionados, introduce IDs la AWS cuenta de las cuentas que quieres configurar. Debe repetir este proceso para cada cuenta nueva si utiliza permisos autogestionados.
     - Introduzca las regiones en las que utilizará CloudWatch Systems Manager.
     - Confirme que la implementación se ha realizado correctamente consultando el estado del conjunto de pilas en la pestaña Operaciones y Instancias apiladas.

- Compruebe que Systems Manager y CloudWatch que funcionen correctamente en las cuentas implementadas siguiendo el paso 7 de la Configuración rápida personalizada en una sola cuenta y región con una CloudFormation pila sección de esta guía.

Consideraciones para configurar los servidores locales

El CloudWatch agente para los servidores locales y las máquinas virtuales se instala y configura mediante un enfoque similar al de las instancias EC2. Sin embargo, en la siguiente tabla se incluyen las consideraciones que debe tener en cuenta al instalar y configurar el CloudWatch agente en servidores locales y. VMs

Dirija al CloudWatch agente a las mismas credenciales temporales utilizadas para Systems Manager.	Al configurar Systems Manager en un entorno híbrido que incluye servidores locales, puede activar Systems Manager con una función de IAM. Debe usar el rol creado para las instancias de EC2, que incluye las `CloudWatchAgentServerPolicy` políticas y. `AmazonSSMManagedInstanceCore` Esto hace que el agente de Systems Manager recupere y escriba las credenciales temporales en un archivo de credenciales local. Puede apuntar la configuración del CloudWatch agente al mismo archivo. Puede usar el proceso de Configurar servidores locales que usan el agente de Systems Manager y el CloudWatch agente unificado para usar solo credenciales temporales en el AWS Knowledge Center. También puede automatizar este proceso definiendo un manual de automatización de Systems Manager y una asociación de State Manager independientes, y segmentando sus instancias locales con etiquetas. Al crear una activación de Systems Manager para sus

	instancias locales, debe incluir una etiqueta que identifique las instancias como instancias locales.
Considere la posibilidad de utilizar cuentas y regiones que tengan VPN o Direct Connect acceso y. AWS PrivateLink	Puede usar AWS Direct Connect o AWS Virtual Private Network (Site-to-Site VPN) para establecer conexiones privadas entre las redes locales y su nube privada virtual (VPC). AWS PrivateLinkestablece una conexión privada a CloudWatch los registros con un punto final de VPC de interfaz. Este enfoque resulta útil si tiene restricciones que impiden que los datos se envíen a través de la Internet pública a un punto final de servicio público.
Todas las métricas deben incluirse en el archivo CloudWatch de configuración.	Amazon EC2 incluye métricas estándar (por ejemplo, el uso de la CPU), pero estas métricas deben definirse para las instancias locales. Puede utilizar un archivo de configuración de plataforma independiente para definir estas métricas para los servidores locales y, a continuación, añadir la configuración a la configuración de CloudWatch métricas estándar de la plataforma.

Consideraciones sobre las instancias EC2 efímeras

Las instancias EC2 son temporales o efímeras si las aprovisionan Amazon EC2 Auto Scaling, Amazon EMR, Amazon EC2 Spot Instances o. AWS Batch Las instancias EC2 efímeras pueden generar una gran cantidad 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 añadir información contextual dinámica adicional en los nombres de los grupos de registros y de las secuencias de registro. Por ejemplo, puede incluir el ID de solicitud de la instancia puntual, el nombre del clúster de Amazon EMR o el nombre del grupo de Auto Scaling. Esta información puede variar en el caso de las instancias EC2 recién lanzadas y es posible que tenga que recuperarla y configurarla en tiempo de ejecución. Para

ello, escriba un archivo de configuración del CloudWatch agente durante el arranque y reinicie el agente para incluir el archivo de configuración actualizado. Esto permite la entrega de registros y métricas para CloudWatch utilizar información dinámica sobre el tiempo de ejecución.

También debe asegurarse de que el CloudWatch agente envíe las métricas y los registros antes de que se cancelen las instancias efímeras de EC2. El CloudWatch agente incluye un `flush_interval` parámetro que se puede configurar para definir el intervalo de tiempo para vaciar los búferes de registros y métricas. Puede reducir este valor en función de la carga de trabajo, detener el CloudWatch agente y forzar a que los búferes se vacíen antes de que finalice la instancia de EC2.

Uso de una solución automatizada para implementar el agente CloudWatch

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:

- Compruebe que la automatización abarque las versiones del sistema operativo compatibles OSs y las que son compatibles. Si el script de automatización no es compatible con todos los de su organización OSs, debe definir soluciones alternativas para las no compatibles OSs.
- Compruebe que la solución de automatización compruebe periódicamente si hay actualizaciones y mejoras de los CloudWatch agentes. La solución de automatización debe comprobar periódicamente si hay actualizaciones del CloudWatch agente o desinstalar y volver a instalar el agente con regularidad. Puede utilizar la funcionalidad de un programador o de una solución de automatización para comprobar y actualizar el agente con regularidad.
- Compruebe que puede confirmar el cumplimiento de la instalación y la configuración del agente. Su solución de automatización debería permitirle determinar cuándo un sistema no tiene el agente instalado o cuándo el agente no funciona. Puede implementar una notificación o una alarma en su solución de automatización para realizar un seguimiento de las instalaciones y configuraciones fallidas.

Despliegue del CloudWatch agente durante el aprovisionamiento de la instancia con el script de datos de usuario

Puede usar este enfoque si no planea usar Systems Manager y quiere usarlo de forma selectiva CloudWatch para sus instancias de EC2. Por lo general, este enfoque se utiliza una sola vez

o cuando se requiere una configuración especializada. AWS proporciona enlaces directos al CloudWatch agente que se pueden descargar en los scripts de inicio o de datos de usuario. Los paquetes de instalación del agente se pueden ejecutar de forma silenciosa sin la interacción del usuario, lo que significa que puede utilizarlos en despliegues automatizados. Si utiliza este enfoque, debe tener en cuenta las siguientes consideraciones:

- Aumenta el riesgo de que los usuarios no instalen el agente ni configuren las métricas estándar. Los usuarios pueden aprovisionar las instancias sin incluir los pasos necesarios para instalar el CloudWatch agente. También podrían configurar mal el agente, lo que podría provocar incoherencias en el registro y la supervisión.
- Los scripts de instalación deben ser específicos del sistema operativo y ser adecuados para las diferentes versiones del sistema operativo. Necesitará scripts independientes si pretende utilizar tanto Windows como Linux. El script de Linux también debe tener diferentes pasos de instalación en función de la distribución.
- Debe actualizar periódicamente el CloudWatch agente con nuevas versiones cuando estén disponibles. Esto se puede automatizar si usas Systems Manager con State Manager, pero también puedes configurar el script de datos de usuario para que se vuelva a ejecutar al iniciar la instancia. A continuación, el CloudWatch agente se actualiza y se vuelve a instalar cada vez que se reinicia.
- Debe automatizar la recuperación y la aplicación de las configuraciones estándar 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 durante el arranque y reiniciar el CloudWatch agente.

Incluir el CloudWatch agente en su AMIs

La ventaja de utilizar este enfoque es que no tiene que esperar a que se instale y configure el CloudWatch agente, y puede empezar inmediatamente a registrar y supervisar. Esto le ayuda a supervisar mejor los pasos de aprovisionamiento e inicio de las instancias en caso de que las instancias no se inicien. Este enfoque también es adecuado si no tiene previsto utilizar el agente de Systems Manager. Si utiliza este enfoque, debe tener en cuenta las siguientes consideraciones:

- Debe existir un proceso de actualización porque es AMIs posible que no incluya la versión más reciente del CloudWatch agente. El 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 de forma regular y cuando se aprovisione la instancia EC2. Si utiliza Systems Manager, puede

utilizar la Instalación del CloudWatch agente mediante Systems Manager Distributor y State Manager solución que se proporciona en esta guía para ello. Si no utilizas Systems Manager, puedes usar un script de datos de usuario para actualizar el agente al iniciar y reiniciar la instancia.

- El archivo de configuración del CloudWatch 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 durante el arranque y, a continuación, reiniciar el CloudWatch agente.
- El CloudWatch agente debe reiniciarse después de actualizar la CloudWatch configuración.
- AWS las credenciales no deben guardarse en la AMI. Asegúrese de que no haya AWS credenciales locales almacenadas en la AMI. Si usa Amazon EC2, puede aplicar la función de IAM necesaria a su instancia y evitar las credenciales locales. Si usa instancias locales, debe automatizar o actualizar manualmente las credenciales de la instancia antes de iniciar el agente. CloudWatch

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
- Registros de contenedores de Amazon ECS para los tipos de lanzamiento de EC2 y Fargate
- Uso del enrutamiento de registros personalizado con FireLens Amazon ECS
- Métricas de Amazon ECS

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 Consola de administración de AWS para aprovisionar un clúster de Amazon ECS con el tipo de lanzamiento EC2, lo que crea una 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 del CloudWatch agente mediante 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 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 el agente de contenedor AMIs y optimizado más reciente de 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 AMI optimizada más recientemente del almacén de parámetros

mediante el formato de parámetros del almacén de parámetros optimizado para Amazon ECS AMIs. 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 CloudFormation plantillas.

AWS proporciona los mismos parámetros del almacén de parámetros en cada región compatible. Esto significa que 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 la versión más reciente de Amazon ECS AMIs 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`,`syslog`, o`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`, `ysplunk`. `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. Consola de administración de AWS `/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 registro	`/<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 utiliza un CI/CD) pipeline or automated process, you can create a new task definition revision for your application with each new Docker image build. For example, you can include the Docker image name, image tag, GitHub revision, or other important information in your task definition revision and logging configuration as a part of your CI/CD proceso de integración y entrega continuas.

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 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 Configure State Manager y Distributor para el despliegue y la configuración de los CloudWatch 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 CloudWatch integra con Logs para el plano de control de Kubernetes. Amazon EKS proporciona el plano de control como un servicio gestionado y puede activar el registro sin necesidad de instalar un CloudWatch agente. El CloudWatch agente también se puede implementar para capturar los registros de nodos y contenedores de Amazon EKS. Fluent Bit y Fluentd también son compatibles para enviar los registros de los contenedores a CloudWatch Logs.

CloudWatch Container Insights proporciona una solución integral de monitoreo de métricas para Amazon EKS a nivel de clúster, nodo, pod, tarea y servicio. Amazon EKS también admite varias opciones de captura de métricas con Prometheus. El plano de control de Amazon EKS proporciona un punto final de métricas que expone las métricas en formato Prometheus. Puede implementar Prometheus en su clúster de Amazon EKS para consumir estas métricas.

También puedes configurar el CloudWatch agente para recopilar y CloudWatch crear métricas de Prometheus, además de consumir otros puntos de conexión de Prometheus. La supervisión de Container Insights para Prometheus también puede descubrir y capturar automáticamente las métricas de Prometheus de las cargas de trabajo y los sistemas en contenedores compatibles.

Puede instalar y configurar el 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 para Amazon EKS

El registro de Kubernetes se puede dividir en registro del plano de control, registro de nodos y registro de aplicaciones. El plano de control de Kubernetes es un conjunto de componentes que administran los clústeres de Kubernetes y producen registros que se utilizan con fines de auditoría y diagnóstico. Con Amazon EKS, puede activar los registros de distintos componentes del plano de control y enviarlos a CloudWatch.

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

Los contenedores se agrupan como pods dentro de un clúster de Kubernetes y están programados para ejecutarse en los nodos de Kubernetes. La mayoría de las aplicaciones contenerizadas escriben en base a la salida estándar y al error estándar, y el motor de contenedores redirige la salida a un controlador de registro. En Kubernetes, los registros del contenedor se encuentran en el directorio de un nodo. `/var/log/pods` Puede configurar CloudWatch y Container Insights para capturar estos registros para cada uno de sus 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 inquilino y 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 por. AWS Los nodos del plano de control del clúster de Amazon EKS están integrados CloudWatch y puede activar el registro para componentes específicos del plano de control.

Se proporcionan registros para cada instancia de componente del plano de control de Kubernetes. AWS gestiona el estado de los nodos del plano de control y proporciona un acuerdo de nivel de servicio (SLA) para el punto final de Kubernetes.

Registro de nodos y aplicaciones de Amazon EKS

Le recomendamos que utilice CloudWatchContainer Insights para capturar registros y métricas para Amazon EKS. Container Insights implementa métricas a nivel de clúster, nodo y pod con el CloudWatch agente y con Fluent Bit o Fluentd para la captura de registros. CloudWatch Container Insights también proporciona paneles automáticos con vistas en capas de las métricas capturadas. CloudWatch Container Insights se implementa como CloudWatch DaemonSet un Fluent Bit DaemonSet que se ejecuta en todos los nodos de Amazon EKS. Container Insights no admite los nodos Fargate porque los administra AWS y no son compatibles. DaemonSets El registro de Fargate para Amazon EKS se describe por separado en esta guía.

La siguiente tabla muestra los CloudWatch grupos de registros y los registros capturados por la configuración de captura de registros predeterminada de Fluentd o Fluent Bit para Amazon EKS.

`/aws/containerinsights/Cluster_Name/application`	Todos los archivos de registro están incluidos. `/var/log/containers` Este directorio proporciona enlaces simbólicos a todos los registros de

	contenedores de Kubernetes de la `/var/log/pods` estructura de directorios. Esto captura los registros del contenedor de aplicaciones que se escriben en o. `stdout` `stderr` También incluye registros de los contenedores del sistema Kubernetes`aws-vpc-cni-init`, como, y`kube-proxy` . `coreDNS`
`/aws/containerinsights/Cluster_Name/host`	Registros de`/var/log/dmesg` , y`/var/log/secure` . `/var/log/messages`
`/aws/containerinsights/Cluster_Name/dataplane`	Los registros en `/var/log/journal` para `kubelet.service` , `kubeproxy.service` y `docker.service` .

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

La siguiente tabla muestra los registros que son específicos de Kubernetes y que debe capturar si no utiliza Container Insights con Fluent Bit o Fluentd para el registro.

`/var/log/containers`	Este directorio proporciona enlaces simbólicos a todos los registros de contenedores de Kubernetes incluidos en la estructura de directorios. `/var/log/pods` Esto captura de manera efectiva los registros del contenedor de aplicaciones que se escriben en o. `stdout` `stderr` Esto incluye los registros de los contenedores del sistema Kubernetes`aws-vpc-cni-init` , como, y`kube-proxy` .

	`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 encuentran aquí

Debe asegurarse de que los nodos de Amazon EKS instalen y configuren el CloudWatch agente para enviar los registros y las métricas correspondientes a nivel del sistema. Sin embargo, la AMI optimizada para Amazon EKS no incluye el agente Systems Manager. Al usar plantillas de lanzamiento, puede automatizar la instalación del agente de Systems Manager y una CloudWatch configuración predeterminada que captura registros importantes específicos 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 como grupo de nodos gestionado o como nodos autogestionados.

Con los grupos de nodos gestionados, se proporciona una plantilla de lanzamiento que incluye la sección de datos de usuario para automatizar la instalación y CloudWatch configuración del agente de Systems Manager. Puede personalizar y utilizar la plantilla amazon_eks_managed_node_group_launch_config.yaml para crear una CloudFormation plantilla de lanzamiento que instale el agente y el agente de Systems Manager y que también añada una configuración de registro específica de Amazon EKS al directorio de configuración. CloudWatch CloudWatch Esta plantilla se puede utilizar para actualizar la plantilla de lanzamiento de grupos de nodos gestionados por Amazon EKS con un enfoque infrastructure-as-code (IaC). Cada actualización de la CloudFormation plantilla incluye una nueva versión de la plantilla de lanzamiento. A continuación, puede actualizar el grupo de nodos para usar la nueva versión de la plantilla y hacer que el proceso de ciclo de vida gestionado actualice sus nodos sin tiempo de inactividad. Asegúrese de que la función de IAM y el perfil de instancias aplicados a su grupo de nodos gestionado incluyan las políticas `AmazonSSMManagedInstanceCore` AWS gestionadas `CloudWatchAgentServerPolicy` y las políticas gestionadas.

Con los nodos autogestionados, puede aprovisionar y gestionar directamente el ciclo de vida y la estrategia de actualización de sus nodos de Amazon EKS. Los nodos autogestionados le permiten ejecutar nodos de Windows en el clúster de Amazon EKS y en Bottlerocket, entre otras opciones. Puede utilizarlos CloudFormation para implementar nodos autogestionados en sus clústeres de Amazon EKS, lo que significa que puede utilizar un enfoque de IaC y de cambio

gestionado para sus clústeres de Amazon EKS. AWS proporciona la CloudFormation plantilla amazon-eks-nodegroup.yaml que puede usar tal cual o personalizar. La plantilla proporciona todos los recursos necesarios para los nodos de Amazon EKS de un clúster (por ejemplo, una función de IAM independiente, un grupo de seguridad, un grupo de Amazon EC2 Auto Scaling y una plantilla de lanzamiento). La CloudFormation plantilla amazon-eks-nodegroup.yaml es una versión actualizada que instala el agente y el agente de Systems Manager necesarios y, CloudWatch además, añade una configuración de registro específica de Amazon EKS al CloudWatch directorio de configuración.

Cómo iniciar sesión en Amazon EKS en Fargate

Con Amazon EKS en Fargate, puede implementar pods sin asignar ni administrar los nodos de Kubernetes. Esto elimina la necesidad de capturar registros a nivel de sistema para sus nodos de Kubernetes. Para capturar los registros de sus cápsulas Fargate, puede usar Fluent Bit para reenviar los registros directamente a. CloudWatch Esto te permite enrutar automáticamente los registros a un contenedor lateral para tus cápsulas Amazon EKS en Fargate CloudWatch sin necesidad de configuración adicional. Para obtener más información al respecto, consulte el registro de Fargate en la documentación de Amazon EKS y Fluent Bit para Amazon EKS en el AWS blog. Esta solución captura las transmisiones `STDOUT` y `STDERR` input/output (E/S) de su contenedor y las envía a CloudWatch través de Fluent Bit, según la configuración de Fluent Bit establecida para el clúster 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, el uso de la CPU y la memoria de los nodos y los pods), pero la API solo proporciona point-in-time información y no métricas históricas. El servidor de métricas de Kubernetes se suele utilizar para las implementaciones de Amazon EKS y Kubernetes para agregar métricas, proporcionar información histórica a corto plazo sobre las métricas y admitir funciones como Horizontal Pod Autoscaler.

Amazon EKS expone las métricas del plano de control a través del servidor API de Kubernetes en formato Prometheus y puede capturar e ingerir estas métricas. CloudWatch CloudWatch y Container Insights también se pueden configurar para proporcionar una captura integral de métricas, análisis y alarmas 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 punto final de la API HTTP. `/metrics` Deberías instalar Prometheus en tu clúster de Kubernetes para graficar y ver estas métricas con un navegador web. También puedes incorporar las métricas expuestas por el servidor API de Kubernetes. CloudWatch

Métricas de nodos y sistemas para Kubernetes

Kubernetes proporciona el pod del servidor de métricas Prometheus que puede implementar y ejecutar en sus clústeres de Kubernetes para obtener estadísticas de CPU y memoria a nivel de clúster, nodo y pod. Estas métricas se utilizan con el escalador automático de pod horizontal y el escalador automático de pod vertical. CloudWatch también puede proporcionar estas métricas.

Deberías instalar el servidor de métricas de Kubernetes si utilizas el panel de control de Kubernetes o los escaladores automáticos de los módulos horizontal y vertical. El panel de control de Kubernetes te ayuda a buscar y configurar el clúster, los nodos, los pods y la configuración relacionada de Kubernetes, así como a ver las métricas de CPU y memoria del Kubernetes Metrics Server.

Las métricas proporcionadas por el servidor de métricas de Kubernetes no se pueden usar para fines que no sean de escalado automático (por ejemplo, monitoreo). Las métricas están pensadas para el point-in-time análisis y no para el análisis histórico. El panel de control de Kubernetes lo implementa `dashboard-metrics-scraper` para almacenar las métricas del 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 detectar todos los contenedores en ejecución de un clúster y proporcionar métricas a nivel de nodo. Recopila datos de rendimiento en cada capa del conjunto de rendimiento. Puede utilizar el Quick Start desde AWS Quick Starts o configurar Container Insights por separado. El Quick Start configura el monitoreo de métricas con el CloudWatch agente y el registro con Fluent Bit, por lo que solo necesita implementarlo una vez para el registro y la supervisión.

Como los nodos de Amazon EKS son instancias EC2, debe capturar las métricas a nivel de sistema, además de las métricas capturadas por Container Insights, utilizando los estándares que definió para Amazon EC2. Puede utilizar el mismo enfoque de la Configure State Manager y Distributor para el despliegue y la configuración de los CloudWatch agentes sección de esta guía para instalar y configurar el CloudWatch agente para sus clústeres de Amazon EKS. Puede actualizar su archivo de CloudWatch configuración específico de Amazon EKS para incluir las métricas y la configuración de registro específica de Amazon EKS.

El CloudWatch agente con el soporte de Prometheus puede descubrir y extraer automáticamente las métricas de Prometheus de las cargas de trabajo y los sistemas compatibles y en contenedores. Las ingiere como CloudWatch registros en formato métrico integrado para analizarlos con Logs Insights y crea métricas automáticamente. CloudWatch CloudWatch

> **Important**
>
> Debes implementar una versión especializada del CloudWatch agente para recopilar las métricas de Prometheus. Se trata de un agente independiente del CloudWatch agente desplegado para Container Insights. Puede usar la aplicación Java de ejemplo prometheus_jmx, que incluye los archivos de implementación y configuración del agente CloudWatch y la implementación del pod de Amazon EKS para demostrar el descubrimiento de métricas de Prometheus. Para obtener más información, consulte Configurar Java/JMX una carga de trabajo de ejemplo en Amazon EKS y Kubernetes en la documentación. CloudWatch También puede configurar el CloudWatch agente para que capture métricas de otros objetivos de Prometheus que se ejecuten en su clúster de Amazon EKS.

Métricas de aplicación

Puede crear sus propias métricas personalizadas con el formato de métricas CloudWatch integrado. Para incorporar declaraciones en formato métrico integrado, debe enviar las entradas en formato métrico integrado a un punto final con formato métrico integrado. El CloudWatch agente se puede configurar como un contenedor sidecar en su cápsula Amazon EKS. La configuración del CloudWatch agente se almacena en Kubernetes ConfigMap y el contenedor sidecar del CloudWatch agente la lee para iniciar el punto final con formato métrico integrado.

También puede configurar su aplicación como un objetivo de Prometheus y configurar el agente, con CloudWatch la ayuda de Prometheus, para que descubra, extraiga e incorpore sus métricas. CloudWatch Por ejemplo, puede usar el exportador JMX de código abierto con sus aplicaciones Java para exponer los JMX Beans para que el agente los consuma en Prometheus. CloudWatch

Si no desea utilizar el formato de métricas integrado, también puede crear y actualizar CloudWatch métricas mediante la API o el SDK.AWSAWS Sin embargo, no recomendamos este enfoque porque combina la supervisión y la lógica de la aplicación.

Métricas de Amazon EKS en Fargate

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

- DaemonSets no son compatibles actualmente. Container Insights se implementa ejecutando el CloudWatch agente como si fuera DaemonSet en cada nodo del clúster.
- HostPath no se admiten los volúmenes persistentes. El contenedor del CloudWatch agente usa los volúmenes persistentes de HostPath como requisito previo para recopilar los datos métricos del contenedor.
- Fargate evita los contenedores privilegiados y el acceso a la información del host.

Puede usar el router de registro integrado para que Fargate envíe declaraciones en formato métrico integradas a. CloudWatch El router de registros usa Fluent Bit, que tiene un CloudWatch complemento que se puede configurar para admitir sentencias de formato métrico integradas.

Puede recuperar y capturar métricas a nivel de pod para sus nodos de Fargate implementando el servidor Prometheus en su clúster de Amazon EKS para recopilar métricas de sus nodos de Fargate. Como Prometheus requiere almacenamiento persistente, puede implementar Prometheus en Fargate si utiliza Amazon Elastic File System (Amazon EFS) para el almacenamiento persistente. También puede implementar Prometheus en un nodo respaldado por Amazon EC2. Para obtener más información, consulte Monitorización de Amazon EKS sobre el AWS Fargate uso de Prometheus y Grafana en el blog. AWS

Supervisión de Prometheus en Amazon EKS

Amazon Managed Service for Prometheus proporciona un servicio escalable, seguro AWS y gestionado para Prometheus de código abierto. Puede usar el lenguaje de consultas Prometheus (ProMQL) para monitorear el rendimiento de las cargas de trabajo en contenedores sin administrar la infraestructura subyacente para la ingesta, el almacenamiento y la consulta de métricas operativas. Puede recopilar métricas de Prometheus de Amazon EKS y Amazon ECS AWS utilizando servidores Distro OpenTelemetry for (ADOT) o Prometheus como agentes de recopilación.

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

- Amazon Managed Service for Prometheus le permite utilizar los servidores Prometheus existentes desplegados en Amazon EKS o Kubernetes autogestionados y configurarlos para que escriban en Amazon Managed Service for Prometheus en lugar de en un almacén de datos configurado localmente. Esto elimina el trabajo pesado e indiferenciado que supone gestionar un almacén de datos de alta disponibilidad para sus servidores Prometheus y su infraestructura. Amazon Managed Service for Prometheus es una opción adecuada si tiene una implementación avanzada de Prometheus que desea aprovechar en la nube. AWS
- Grafana apoya directamente a Prometheus como fuente de datos para la visualización. Si quieres usar Grafana con Prometheus en lugar de CloudWatch paneles para la supervisión de tus contenedores, Amazon Managed Service for Prometheus podría cumplir tus requisitos. Amazon Managed Service for Prometheus se integra con Amazon Managed Grafana para proporcionar una solución gestionada de monitorización y visualización de código abierto.
- Prometheus le permite realizar análisis de sus métricas operativas mediante consultas de ProMQL. Por el contrario, el CloudWatch agente ingiere las métricas de Prometheus en formato CloudWatch métrico integrado en los registros, lo que da como resultado las métricas. CloudWatch Puede consultar los registros en formato métrico incrustado mediante CloudWatch Logs Insights.
- Si no planeas usarlo CloudWatch para la supervisión y la captura de métricas, deberías usar Amazon Managed Service for Prometheus con tu servidor Prometheus y una solución de visualización como Grafana. Debe configurar su servidor Prometheus para extraer las métricas de sus objetivos de Prometheus y configurar el servidor para que escriba de forma remota en su

espacio de trabajo de Amazon Managed Service for Prometheus. Si utilizas Amazon Managed Grafana, puedes integrar directamente Amazon Managed Grafana con tu fuente de datos de Amazon Managed Service for Prometheus mediante el complemento incluido. Como los datos de las métricas se almacenan en Amazon Managed Service for Prometheus, no hay que depender CloudWatch del agente ni tener que ingerir datos en él. CloudWatch El CloudWatch agente es obligatorio para la supervisión de Container Insights para Prometheus.

También puedes usar el recopilador de ADOT para extraer datos de una aplicación equipada con Prometheus y enviar las métricas a Amazon Managed Service for Prometheus. Para obtener más información sobre ADOT Collector, consulta la documentación de la Distro.AWS OpenTelemetry

Registro y métricas para AWS Lambda

Lambda elimina la necesidad de gestionar y supervisar los servidores para sus cargas de trabajo y trabaja automáticamente con CloudWatch métricas y CloudWatch registros 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 los CloudWatch registros, sin necesidad de controladores de registro. Lambda también aprovisiona automáticamente los contenedores que ejecutan la función de Lambda y los configura para generar mensajes de registro en flujos de registro independientes.

Las invocaciones posteriores de la función Lambda pueden reutilizar el mismo contenedor y la misma salida 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 Lambda por primera vez. Las funciones Lambda pueden tener varias versiones y usted puede elegir la versión que desee ejecutar. Todos los registros de las invocaciones de la función 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 Lambda. Lambda tiene una convención de nomenclatura estándar para los flujos de registro que utiliza un `YYYY/MM/DD/[<FunctionVersion>]<InstanceId>` formato. `InstanceId`Se genera AWS para identificar la instancia de la función Lambda.

Le recomendamos que formatee sus mensajes de registro en formato JSON porque puede consultarlos más fácilmente con CloudWatch Logs 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 el módulo de registro de Python para 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 el kit de AWS Lambda herramientas para desarrolladores de Powertools for Python para facilitar 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 de 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 establecer variables de entorno para el entorno de ejecución de la función Lambda sin necesidad de actualizar el código. Por ejemplo, puede crear una variable de `LAMBDA_LOG_LEVEL` entorno que defina el nivel de salida del registro que puede recuperar del código. En el siguiente ejemplo, se intenta recuperar una variable de `LAMBDA_LOG_LEVEL` entorno y utilizar el valor para definir la salida del registro. Si la variable de entorno no está establecida, el `INFO` nivel se establece de forma predeterminada.

```
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 Service o una función Lambda) mediante filtros de suscripción. Si no utilizas Amazon OpenSearch Service, puedes usar una función de Lambda para procesar los registros y enviarlos al AWS servicio que elijas mediante. AWS SDKs

También puede utilizarla SDKs para destinos de registro fuera de la AWS nube en su función 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 el acoplamiento de la lógica operativa a la función Lambda.

Métricas de función de Lambda

Lambda le permite ejecutar el código sin administrar ni escalar los servidores, lo que prácticamente elimina la carga de la auditoría y el diagnóstico a nivel del sistema. Sin embargo, sigue siendo importante entender 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 Lambda también tienen métricas a nivel de aplicación que deben capturarse y analizarse. Lambda admite directamente el formato de métrica integrado para facilitar la captura de métricas a nivel de aplicación. CloudWatch

Métricas a nivel de sistema

Lambda se integra automáticamente con CloudWatch Metrics y proporciona un conjunto de métricas estándar para las 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.

Los errores de invocación impiden 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 múltiples invocaciones de la función.

Una función Lambda que se invoca correctamente devuelve una respuesta HTTP 200 incluso si la función lanza una excepción. Las funciones de Lambda deben implementar la gestión de errores y generar excepciones para que la `Errors` métrica capture e identifique las ejecuciones fallidas de la función de Lambda. Debe devolver una respuesta formateada a las invocaciones de la función

Lambda que incluya información para determinar si la ejecución ha fallado total, parcialmente o se ha realizado correctamente.

CloudWatch proporciona información de CloudWatch Lambda que puede habilitar para una función de 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 y resolver los problemas rápidamente.

Lambda Insights utiliza el formato métrico integrado para emitir automáticamente información de rendimiento al grupo de `/aws/lambda-insights/` 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 los paneles automáticos. CloudWatch 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 las `memory_utilization` que ayudan a dimensionar correctamente las funciones de Lambda para evitar pagar por capacidad innecesaria.

Métricas de aplicación

También puede crear y capturar las métricas de su propia aplicación CloudWatch mediante el formato de métricas integrado. Puede aprovechar las bibliotecas AWS proporcionadas para el formato métrico integrado para crear y emitir sentencias en formato métrico integrado CloudWatch. La función de CloudWatch registro Lambda integrada está configurada para procesar y extraer sentencias de formato métrico integradas con el formato adecuado.

Búsqueda y análisis de los registros CloudWatch

Después de capturar los registros y las métricas en un formato y una ubicación uniformes, puede buscarlos y analizarlos para mejorar la eficiencia operativa, además de identificar y solucionar los problemas. Le recomendamos que capture sus registros en un formato bien formado (por ejemplo, JSON) para facilitar la búsqueda y el análisis de los registros. La mayoría de las cargas de trabajo utilizan un conjunto de AWS recursos, como la red, el procesamiento, el almacenamiento y las bases de datos. Siempre que sea posible, debe analizar de forma colectiva las métricas y los registros de estos recursos y correlacionarlos para supervisar y gestionar de forma eficaz todas sus AWS cargas de trabajo.

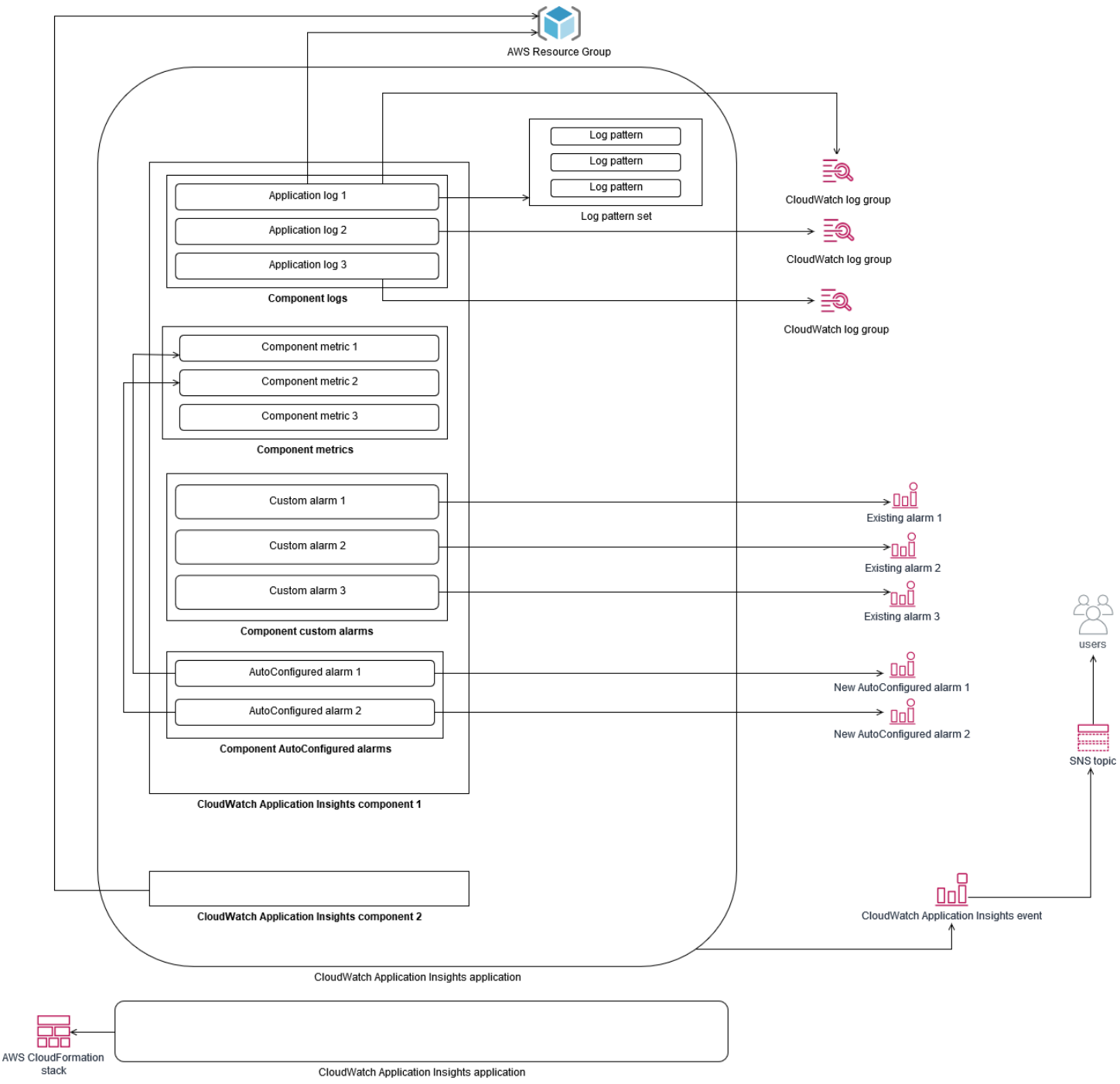
CloudWatch ofrece varias funciones que ayudan a analizar los registros y las métricas, como CloudWatch Application Insights, que permite definir y supervisar de forma colectiva las métricas y los registros de una aplicación en distintos AWS recursos, la detección de CloudWatch anomalías, que permite detectar anomalías en las métricas, y CloudWatch Log Insights, que permite buscar y analizar de forma interactiva los datos de registro en Logs. CloudWatch

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

Los propietarios de las 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 de la supervisión estándar a nivel de sistema configurada para todas las cargas de trabajo de una cuenta. Configurar la supervisión mediante CloudWatch Application Insights también puede ayudar a los equipos de aplicaciones a adaptarse de forma proactiva a las operaciones y a 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 las aplicaciones. También proporciona un marco basado en componentes que ayuda a los equipos a dividir las responsabilidades de registro y supervisión.

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.

En el caso de los registros, usted define el conjunto de patrones de registro que debe usarse para el componente y dentro de la 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 para determinar cuándo se detecta el patrón. En el caso de las métricas, puede elegir las métricas que desea supervisar para cada componente de una lista de métricas compatibles y específicas del servicio. En el caso de las alarmas, CloudWatch Application Insights crea y configura automáticamente las alarmas estándar o de detección de anomalías para las métricas que se están monitoreando. 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 supervisión. Cada componente ha definido sus propios registros y métricas para CloudWatch supervisarlos mediante registros y métricas.



Las instancias EC2 monitoreadas por CloudWatch Application Insights requieren Systems Manager, CloudWatch agentes y permisos. Para obtener más información al respecto, consulte los requisitos previos para configurar una aplicación con CloudWatch Application Insights en la CloudWatch documentación. CloudWatch Application Insights usa 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 añada un archivo de configuración de CloudWatch agentes independiente al directorio de configuración de CloudWatch agentes 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 de CloudWatch 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 la aplicación están estructurados en formato JSON, CloudWatch Logs Insights descubre automáticamente los campos JSON de los flujos de registros de varios grupos de registros. Puede usar CloudWatch Logs Insights para analizar los registros de las aplicaciones y del sistema, lo que guarda las consultas para usarlas en el futuro. La sintaxis de consulta de CloudWatch Logs Insights admite funciones como la agregación con funciones como sum (), avg (), count (), min () y max (), que pueden resultar útiles para solucionar problemas en las aplicaciones o para analizar el rendimiento.

Si utiliza el formato de métrica integrado para crear CloudWatch métricas, puede consultar sus registros en formato métrico integrado 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 resulta especialmente eficaz para las dimensiones con una alta cardinalidad que generarían un gran número 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 de métrica incrustada solo genera un conjunto limitado de CloudWatch métricas a partir de los datos de métricas que se capturan en la declaración de formato de métrica integrada:

```
{
 "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, puedes ejecutar la siguiente consulta para ver los últimos 20 pods con errores en la 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 datos de CloudWatch registro de 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, después, ampliarlo con Amazon OpenSearch Service para los siguientes casos de uso:

- Control de acceso a los datos detallado: Amazon OpenSearch Service te permite limitar el acceso a los datos al nivel de campo y ayuda a anonimizar los datos de los campos en función de los permisos de los usuarios. Esto resulta útil si deseas obtener asistencia para solucionar 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 común de Amazon OpenSearch Service. Sus equipos de operaciones centralizados pueden analizar las tendencias y los 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: puede utilizar componentes de su pila de aplicaciones y tecnología OSs que no sean compatibles con el CloudWatch agente. Es posible que también desee enriquecer y transformar los datos de registro antes de enviarlos a su solución de registro. Amazon OpenSearch Service es compatible con los clientes estándar de Elasticsearch, como los transportistas de datos de la familia Elastic Beats y Logstash, que admiten el enriquecimiento y la transformación de los registros antes de enviarlos a Amazon Service. OpenSearch
- La solución de administración de operaciones existente utiliza una ElasticSearch pila de Logstash y Kibana (ELK) para el registro y la supervisión. Es posible que ya tenga una inversión significativa en Amazon OpenSearch Service o en 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 utilizándolos.

Si no piensas usar CloudWatch registros, puedes usar agentes, controladores de registros y bibliotecas compatibles con Amazon OpenSearch Service (por ejemplo, Fluentd, Logstash y Open Distro for ElasticSearch API) para enviar tus registros directamente a Amazon Service y omitirlos. OpenSearch CloudWatch Sin embargo, también deberías implementar una solución para capturar los registros generados por los servicios. AWS CloudWatch Los registros son la principal solución de captura de registros para muchos AWS servicios y varios servicios crean automáticamente nuevos grupos de registros 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. Puedes configurar manualmente un filtro de

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

Deberías considerar la posibilidad de configurar un ElasticSearch clúster en una cuenta centralizada o compartida para agregar los registros entre tus cuentas, regiones y aplicaciones. Por ejemplo, AWS Control Tower configura una cuenta de archivo de registros que se utiliza para el registro centralizado. Cuando se crea una cuenta nueva en AWS Control Tower, sus AWS CloudTrail AWS Config registros se envían a un bucket de S3 de esta cuenta centralizada. El registro utilizado AWS 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 centralizados de Amazon OpenSearch Service en su cuenta de registro centralizada y configurar grupos de registros en sus otras cuentas para transmitir los registros a los clústeres centralizados de Amazon OpenSearch Service.

Puedes crear clústeres de Amazon OpenSearch Service independientes para gestionar diferentes aplicaciones o capas de tu arquitectura de nube que podrían estar distribuidas entre tus cuentas. El uso de clústeres de Amazon OpenSearch Service independientes le ayuda a reducir el riesgo 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 único y automatizado de las métricas importantes le ayuda a detectar y resolver los problemas antes de que afecten a sus cargas de trabajo. CloudWatch facilita la representación gráfica y la comparación de varias métricas mediante el uso de varias estadísticas durante un período de tiempo específico. Puede utilizarla CloudWatch para buscar en todas las métricas con los valores de dimensión necesarios para encontrar las métricas que necesita para su análisis.

Le recomendamos que comience su enfoque de captura de métricas incluyendo un conjunto inicial de métricas y dimensiones para utilizarlas como referencia para supervisar una carga de trabajo. Con el tiempo, la carga de trabajo va madurando y puedes añadir métricas y dimensiones adicionales que te ayuden a analizarla y respaldarla mejor. Sus aplicaciones o cargas de trabajo pueden utilizar varios AWS recursos y tener sus propias métricas personalizadas. Debe agrupar estos recursos en un espacio de nombres para que sea más fácil identificarlos.

También debes tener en cuenta cómo se correlacionan los datos de registro y supervisión para poder identificar rápidamente los datos de registro y supervisión pertinentes para diagnosticar problemas específicos. Puede usar el mapa de AWS X-Ray rastreo para correlacionar los rastreos, las métricas, los registros y las alarmas para diagnosticar problemas. También deberías considerar la posibilidad de incluir dimensiones adicionales en las métricas e identificadores en los registros de tus cargas de trabajo para ayudarte a buscar e identificar rápidamente los problemas en todos los sistemas y servicios.

Uso de CloudWatch alarmas para monitorizar y emitir alarmas

Puede usar CloudWatch las alarmas para reducir la supervisión manual de sus cargas de trabajo o aplicaciones. Debe empezar por revisar las métricas que está recopilando para cada componente de la carga de trabajo y determinar los umbrales adecuados para cada métrica. Asegúrese de identificar a qué miembros del equipo se les debe notificar cuando se supere un umbral. Debes establecer grupos de distribución y dirigirte a ellos, en lugar de a miembros individuales del equipo.

CloudWatch las alarmas se pueden integrar con su solución de administración de servicios para crear automáticamente nuevos tickets y ejecutar flujos de trabajo operativos. Por ejemplo, AWS proporciona el conector de administración de AWS servicios para ServiceNowayudarle AWS Service Management Connectora configurar rápidamente las integraciones. Este enfoque es fundamental para garantizar que las alarmas emitidas se reconozcan y se ajusten a los flujos de trabajo de operaciones existentes, que tal vez ya estén definidos en estos productos.

También puede crear varias alarmas para la misma métrica que tengan distintos umbrales y períodos de evaluación, lo que ayuda a establecer un proceso de escalamiento. Por ejemplo, si tienes una `OrderQueueDepth` métrica que hace un seguimiento de los pedidos de los clientes, puedes definir un umbral inferior durante un breve período medio de un minuto para avisar a los miembros del equipo de la aplicación por correo electrónico o Slack. También puedes definir otra alarma para la misma métrica durante un período más largo de 15 minutos y con el mismo umbral, que envíe páginas, correos electrónicos y notifique 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 notifique a la alta dirección y a todos los miembros del equipo que hayan recibido la notificación anterior. La creación de varias alarmas le ayuda a tomar diferentes medidas para diferentes condiciones. Puede empezar con un proceso de notificación sencillo y, a continuación, ajustarlo y mejorarlo según sea necesario.

Uso de la detección de CloudWatch anomalías para monitorear y emitir alarmas

Puede utilizar la detección de CloudWatch anomalías si no está seguro de los umbrales que debe aplicar a una métrica concreta o si desea que una alarma ajuste automáticamente los valores límite en función de los valores históricos observados. CloudWatch La detección de anomalías es especialmente útil para las métricas que pueden tener cambios de actividad regulares y predecibles, por ejemplo, si los pedidos de compra diarios que se entregan el mismo día aumentan antes de la hora límite. La detección de anomalías permite establecer umbrales que se ajustan automáticamente y puede ayudar a reducir las falsas alarmas. Puede habilitar la detección de anomalías para cada métrica y estadística, y configurarla para que se emita una alarma en función de valores CloudWatch atípicos.

Por ejemplo, puede habilitar la detección de anomalías para la `CPUUtilization` métrica y la `AVG` estadística en una instancia EC2. A continuación, 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 diferentes umbrales.

Para obtener más información sobre esta sección, consulte Crear una CloudWatch alarma basada en la detección de anomalías en la documentación. CloudWatch

Alarmante en varias regiones y cuentas

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

En entornos con varias cuentas y regiones, le recomendamos que cree alarmas agregadas para sus cuentas y regiones a fin de supervisar los problemas de las cuentas y las regiones mediante el uso CloudFormation StackSets y la agregación de métricas, como el promedio de `CPUUtilization` todas las instancias de EC2.

También debería considerar la posibilidad de crear alarmas estándar para cada carga de trabajo que esté configurada para las CloudWatch métricas y los registros estándar que capture. Por ejemplo, puede crear una alarma independiente para cada instancia de EC2 que supervise la métrica de uso de la CPU y notifique al equipo central de operaciones cuando el uso medio de la CPU supere el 80% a diario. También puede crear una alarma estándar que supervise diariamente el uso medio de la CPU por debajo del 10%. Estas alarmas ayudan al equipo central de operaciones 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

La creación de un conjunto estándar de alarmas para las instancias de EC2 puede llevar mucho tiempo, ser incoherente y ser propensa a errores. Puede acelerar el proceso de creación de alarmas utilizando la amazon-cloudwatch-auto-alarmssolución para crear automáticamente un conjunto estándar de CloudWatch alarmas para sus instancias de EC2 y crear alarmas personalizadas basadas en las etiquetas de las instancias de EC2. La solución elimina la necesidad de crear alarmas estándar de forma manual y puede resultar útil durante una migración a gran escala de instancias de EC2 que utilice herramientas como: CloudEndure También puede implementar esta solución CloudFormation StackSets para que sea compatible con varias regiones y cuentas. Para

obtener más información, consulte Uso de etiquetas para crear y mantener CloudWatch alarmas de Amazon para instancias de Amazon EC2 en el AWS blog.

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. Puede lograrlo utilizando un enfoque de monitoreo activo con Amazon Route 53 Health Checks y CloudWatch 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 del Sistema de Nombres de Dominio (DNS) público. Las comprobaciones de estado de Route 53 inician las conexiones desde las regiones que especifiques en intervalos de diez o 30 segundos. Puede elegir varias regiones para que se ejecute la revisión de estado, cada revisión de estado se realizará de forma independiente y debe elegir al menos tres regiones. Puede buscar una subcadena específica en el cuerpo de la respuesta de una solicitud HTTP o HTTPS si aparece en los primeros 5120 bytes de datos devueltos para la evaluación del estado. Se considera que una solicitud HTTP o HTTPS está en buen estado si devuelve una respuesta de 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 puntos finales de servicio y desea realizar la misma notificación cuando uno de ellos deje de funcionar correctamente. Si usa Route 53 para DNS, puede configurar Route 53 para que realice una conmutación por error a otra entrada de DNS si una comprobación de estado no funciona correctamente. Para cada carga de trabajo crítica, debería considerar la posibilidad de configurar comprobaciones de estado de Route 53 para los puntos finales externos que son fundamentales para las operaciones normales. Las comprobaciones de estado de Route 53 pueden ayudarle a evitar introducir una lógica de conmutación por error en sus aplicaciones.

CloudWatch synthetics le permite definir un canario como un script para evaluar el estado y la disponibilidad de sus cargas de trabajo. Los canarios son scripts escritos en Node.js o Python y funcionan con protocolos HTTP o HTTPS. Crean funciones de Lambda en la cuenta que usan Node.js o Python como marco. Cada canario que defina puede realizar múltiples llamadas HTTP o HTTPS a distintos puntos de conexión. Esto significa que puedes supervisar el estado de una serie de pasos, como un caso de uso o un punto final con dependencias posteriores. Los canarios crean CloudWatch métricas que incluyen cada uno de los pasos que se ejecutaron para que puedas calcular y medir los distintos pasos de forma independiente. Si bien el desarrollo de los canarios requiere más planificación y esfuerzo 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 su nube privada virtual (VPC), lo que los hace ideales para la supervisión de la disponibilidad cuando no tiene una dirección IP pública para el punto final. También puedes usar canaries para monitorear las cargas de trabajo locales, siempre que tengas conectividad desde la VPC al punto final. Esto es especialmente importante cuando tienes una carga de trabajo que incluye puntos finales que existen en las instalaciones.

Rastreo de aplicaciones con AWS X-Ray

Una solicitud a través de la 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 rastreo de aplicaciones, puede identificar rápidamente la causa raíz de los problemas en las aplicaciones que utilizan componentes y servicios distribuidos. Puede utilizarlo AWS X-Raypara rastrear las solicitudes de aplicaciones en varios componentes. X-Ray toma muestras y visualiza las solicitudes en un gráfico de servicio cuando recorren 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 pasa por varios componentes, lo que lo ayuda a ver la solicitud de principio a fin. Puede mejorarlo aún más al incluir 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 terminal de su aplicación con X-Ray. X-Ray se implementa en el código de su aplicación al hacer llamadas al servicio de X-Ray. X-Ray también está AWS SDKs disponible en varios idiomas, incluidos los clientes instrumentados que envían automáticamente los datos a X-Ray. Los X-Ray SDKs proporcionan parches para bibliotecas comunes que se utilizan para realizar llamadas a otros servicios (por ejemplo, HTTP, MySQL, PostgreSQL o MongoDB).

X-Ray proporciona un daemon de X-Ray que puede instalar y ejecutar en Amazon EC2 y Amazon ECS para retransmitir datos a X-Ray. X-Ray crea trazas para su aplicación que capturan los datos de rendimiento de los servidores y contenedores que ejecutan el daemon de X-Ray que atendió la solicitud. X-Ray configura automáticamente sus llamadas a AWS servicios, como Amazon DynamoDB, como subsegmentos mediante la aplicación de parches al SDK. AWS 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 de X-Ray ni instrumentar el código, puede crear subsegmentos para agrupar las llamadas a los servicios externos. X-Ray correlaciona CloudWatch los registros y las métricas con los seguimientos de las aplicaciones si los utiliza AWS X-Ray SDK para Java, lo que significa que puede analizar rápidamente las métricas y los registros relacionados para las solicitudes.

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

Debe instalar y ejecutar el daemon X-Ray en las instancias EC2 en las que se ejecutan los componentes o microservicios de la aplicación. Puede utilizar un script de datos de usuario para implementar el daemon X-Ray cuando se aprovisionen instancias EC2 o puede incluirlo en el proceso de creación de la AMI si crea sus propias AMI. Esto puede resultar especialmente útil cuando las instancias EC2 son efímeras.

Debe usar State Manager para asegurarse de que el daemon X-Ray esté instalado de forma coherente en las instancias de EC2. Para las instancias Windows de Amazon EC2, puede utilizar el RunPowerShellScript documento Systems Manager AWS: para ejecutar el script de Windows que descarga e instala el agente X-Ray. Para las instancias EC2 en Linux, puede usar el RunShellScript documento AWS- para ejecutar el script de Linux que descarga e instala el agente como un servicio.

Puede utilizar el RunRemoteScript documento Systems Manager AWS- para ejecutar el script en un entorno con varias cuentas. Debe crear un bucket de S3 al que pueda acceder desde todas sus cuentas y, si lo utiliza, le recomendamos que cree un bucket de S3 con una política de bucket basada en la organización. AWS Organizations A continuación, cargue los scripts en el depósito de S3, pero asegúrese de que el rol de IAM de sus instancias de EC2 tenga permiso para acceder al depósito y a los scripts.

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

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

Puede implementar el daemon X-Ray como un contenedor sidecar para cargas de trabajo basadas en contenedores, como Amazon ECS o Amazon EKS. Los contenedores de aplicaciones se pueden conectar entonces al contenedor sidecar mediante enlace de contenedores si usa Amazon ECS, o el contenedor puede conectarse directamente al contenedor sidecar en localhost si usa el modo de red awsvpc.

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

Configuración de Lambda para rastrear las solicitudes a X-Ray

La aplicación puede incluir llamadas a funciones de Lambda. No necesita instalar el daemon X-Ray para Lambda porque Lambda administra completamente el proceso daemon y el usuario no puede configurarlo. Puede habilitarla para la función Lambda utilizando Consola de administración de AWS y marcando la opción Active Tracing en la consola de X-Ray.

Para obtener más instrumentación, puede agrupar el SDK de X-Ray con su función Lambda para grabar las llamadas salientes y añadir anotaciones o metadatos.

Instrumentación de sus aplicaciones para X-Ray

Debe evaluar el SDK de X-Ray que se ajusta al lenguaje de programación de la aplicación y clasificar todas las llamadas que la aplicación realiza a otros sistemas. Revisa los clientes que proporciona la biblioteca que has elegido y comprueba si el SDK puede instrumentar automáticamente el seguimiento de la solicitud o respuesta de tu aplicación. Determina si los clientes que proporciona el SDK se pueden usar 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 rastreo.

Cuando instrumente su aplicación, asegúrese de crear anotaciones que le ayuden a identificar y buscar las solicitudes. Por ejemplo, tu aplicación podría usar un identificador para los clientes`customer id`, o segmentar distintos usuarios en función de su función en la aplicación.

Puede crear un máximo de 50 anotaciones para cada rastreo, 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 las anotaciones de forma selectiva para localizar la 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

Al personalizar las reglas de muestreo, puede controlar la cantidad de datos que registra y modificar el comportamiento del muestreo sin modificar ni volver a implementar el código. Las reglas de

muestreo indican al SDK de X-Ray cuántas solicitudes se van a registrar para un conjunto de criterios. De forma predeterminada, el SDK de X-Ray registra la primera solicitud cada segundo y el cinco por ciento de las solicitudes adicionales. 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 la velocidad a la que se muestrean las solicitudes adicionales que superan el tamaño del reservorio.

Debe revisar y actualizar la configuración predeterminada para determinar un valor adecuado para su cuenta. Sus requisitos pueden variar en los entornos de desarrollo, pruebas, pruebas de rendimiento y producción. Es posible que tenga 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 base y volver a evaluar periódicamente si la línea base cumple con sus requisitos.

Cuadros de mando y visualizaciones con CloudWatch

Los paneles le ayudan a centrarse rápidamente en las áreas de interés de las aplicaciones y las cargas de trabajo. CloudWatchproporciona paneles automáticos y también puede crear fácilmente paneles que utilicen métricas. CloudWatch CloudWatch Los paneles proporcionan más información que la visualización de las métricas de forma aislada, ya que ayudan a correlacionar varias métricas e identificar tendencias. Por ejemplo, un panel que incluya los pedidos recibidos, la memoria, el uso de la CPU y las conexiones a la base de datos puede ayudarle a correlacionar los cambios en las métricas de carga de trabajo de varios AWS recursos mientras el número de pedidos aumenta o disminuye.

Debe crear paneles a nivel de cuenta y aplicación para supervisar las cargas de trabajo y las aplicaciones. Para empezar, utilice paneles CloudWatch automáticos, que son paneles de nivel de servicio preconfigurados AWS con métricas específicas del servicio. Los paneles de servicio automáticos muestran todas las métricas estándar del servicio. CloudWatch Los paneles automáticos representan gráficamente todos los recursos utilizados para cada métrica de servicio y te ayudan a identificar rápidamente los recursos atípicos en tu cuenta. Esto puede ayudarlo a identificar los recursos con un uso alto y bajo, lo que puede ayudarlo a optimizar sus costos.

Crear paneles de control multiservicio

Para crear paneles multiservicio, consulte el panel automático de nivel de servicio de un AWS servicio y utilice la opción Añadir al panel del menú Acciones. A continuación, puede añadir métricas de otros paneles automáticos al nuevo panel y eliminar las métricas para limitar el enfoque del panel. También debes añadir tus propias métricas personalizadas para realizar un seguimiento de las observaciones clave (por ejemplo, los pedidos recibidos o las transacciones por segundo). Crear tu propio panel multiservicio personalizado te ayuda a centrarte en las métricas más relevantes para tu carga de trabajo. Le recomendamos que cree paneles multiservicio a nivel de cuenta que abarquen las 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 en un monitor de TV grande en modo de pantalla completa con actualización automática.

Creación de cuadros de mando específicos para aplicaciones o cargas de trabajo

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

Debe evaluar y personalizar periódicamente los paneles de CloudWatch 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 las aplicaciones o cargas de trabajo cuando se introduzcan o retiren funciones. Las actualizaciones de los paneles de control de cargas de trabajo y de aplicaciones específicas deberían ser una actividad obligatoria para la mejora continua de la calidad, además del registro y la supervisión.

Crear paneles de control multicuentas o entre regiones

AWS los recursos son principalmente regionales y las métricas, las alarmas y los paneles son específicos de la región en la que se despliegan los recursos. Esto puede requerir que cambie de región para ver las métricas, los paneles y las alarmas de las cargas de trabajo y las aplicaciones que se encuentran en todas las regiones. Si separa sus aplicaciones y cargas de trabajo en varias cuentas, es posible que también deba volver a autenticarse e iniciar sesión en cada cuenta. Sin embargo, CloudWatch admite la visualización de datos entre cuentas y regiones desde una sola cuenta, lo que significa que puede ver las métricas, las alarmas, los paneles y los 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 las cuentas y los propietarios de los equipos de aplicaciones deben crear paneles de control para las aplicaciones específicas de cada cuenta que se encuentren en distintas regiones a fin de supervisar eficazmente las métricas clave en una ubicación centralizada. CloudWatchLos paneles admiten automáticamente los widgets entre regiones, lo que significa que puede crear un panel que incluya métricas de varias regiones sin necesidad de realizar ninguna configuración adicional.

Una excepción importante es el widget CloudWatch Logs Insights, ya que los datos de registro solo se pueden mostrar de la cuenta y la región en las que esté conectado actualmente. Puede crear

métricas específicas de una región a partir de sus registros mediante filtros de métricas y estas métricas se pueden mostrar en un panel de control que abarque todas las 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 el uso total de la CPU en cada cuenta y región. También puedes usar las matemáticas métricas para agregar y gestionar los datos de varias cuentas y regiones.

Usa la matemática métrica para afinar la observabilidad y las alarmas

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

Sin embargo, AWS proporciona directrices sobre el rendimiento de los volúmenes de Amazon EBS en IOPS. Puede graficar y calcular las IOPS de su volumen de Amazon EBS mediante cálculos métricos sumando `VolumeReadOps` `VolumeWriteOps` y dividiendo por el período elegido para estas métricas.

En este ejemplo, sumamos las IOPS del período y, a continuación, las dividimos por la duración del período para obtener las IOPS. A continuación, puede configurar una alarma en esta expresión matemática métrica para que le avise cuando las IOPS de su volumen se acerquen a la capacidad máxima para ese tipo de volumen. Para obtener más información y ejemplos sobre el uso de la matemática métrica para monitorizar los sistemas de archivos de Amazon Elastic File System (Amazon EFS) con CloudWatch métricas, consulte La matemática CloudWatch métrica de Amazon simplifica la supervisión prácticamente en tiempo real de los sistemas de archivos de Amazon EFS y mucho más en el AWS blog.

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

CloudWatch Container Insights crea paneles automáticos y dinámicos para las cargas de trabajo de contenedores que se ejecutan en Amazon ECS y Amazon EKS. Debe habilitar Container Insights para poder observar la CPU, la memoria, el disco, la red y la información de diagnóstico, como los errores al reiniciar los contenedores. Container Insights genera paneles dinámicos que puede filtrar rápidamente a nivel de clúster, instancia o nodo del contenedor, servicio, tarea, pod y contenedor individual. Container Insights se configura a nivel de clúster y nodo o instancia de contenedor, según el AWS servicio.

Al igual que Container Insights, CloudWatch Lambda Insights crea cuadros de mando dinámicos y automáticos para las funciones de Lambda. Esta solución recopila, agrega y resume las métricas a nivel del sistema, como el tiempo de CPU, la memoria, el disco y la red. También recopila, agrega y resume la información de diagnóstico, como los arranques en frío y las paradas de los trabajadores de Lambda, para ayudarlo a aislar y resolver rápidamente los problemas relacionados con las funciones de Lambda. Lambda está habilitada en el 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 rendimiento, a los rastreos de X-Ray y a un mapa de servicios para visualizar las cargas de trabajo de los contenedores. Ambos utilizan el formato de métricas CloudWatch integrado para capturar CloudWatch métricas y registros de rendimiento.

Puede crear un CloudWatch panel compartido para su carga de trabajo que utilice las métricas capturadas por Container Insights y Lambda Insights. Para ello, filtra y visualiza el panel automático a través de CloudWatch Container Insights y, a continuación, selecciona la opción Añadir al panel de control, que te permite añadir las métricas que se muestran a un CloudWatch panel estándar. A continuación, puede eliminar o personalizar las métricas y añadir otras métricas para representar correctamente su carga de trabajo.

CloudWatch integración con AWS servicios

AWS proporciona muchos servicios que incluyen opciones de configuración adicionales para el registro y las métricas. Estos servicios suelen permitir configurar los registros para la salida de CloudWatch los registros y CloudWatch las métricas para la salida de las métricas. La infraestructura subyacente utilizada para proporcionar estos servicios está gestionada AWS y es inaccesible, pero puede utilizar las opciones de registro y métricas de los servicios aprovisionados para obtener más información y solucionar problemas. Por ejemplo, puede publicar los registros de flujo de la VPC o también puede configurar las instancias de Amazon Relational Database Service (Amazon RDS) para publicar los registros. CloudWatch CloudWatch

La mayoría de AWS los servicios registran sus llamadas a la API con la integración de. AWS CloudTrail CloudTrail también admite la integración con CloudWatch los registros, lo que significa que puede buscar y analizar la actividad en AWS los servicios. También puedes usar Amazon EventBridge para crear y configurar la automatización y las notificaciones con reglas de eventos para acciones específicas realizadas en AWS los servicios. Algunos servicios se integran directamente con EventBridge. También puede crear eventos que se entreguen a través de CloudTrail.

Amazon Managed Grafana para la creación de paneles y la visualización

Amazon Managed Grafana se puede utilizar para observar y visualizar sus AWS cargas de trabajo. Amazon Managed Grafana le ayuda a visualizar y analizar sus datos operativos a escala. Grafana es 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 resulta especialmente útil si su organización ya utiliza Grafana para la visualización de las cargas de trabajo existentes y desea ampliar la cobertura a las cargas de trabajo. AWS Puede utilizar Amazon Managed Grafana CloudWatch añadiéndolo como fuente de datos, lo que significa que puede crear visualizaciones utilizando métricas. CloudWatch Amazon Managed Grafana admite paneles de control AWS Organizations y puede centralizarlos mediante CloudWatch métricas de varias cuentas y regiones.

En la siguiente tabla se muestran las ventajas y consideraciones a tener en cuenta a la hora de utilizar Amazon Managed Grafana en lugar de CloudWatch utilizar dashboards. 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 las 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, incluidas las métricas. CloudWatch Amazon Managed Grafana incluye una serie de fuentes de datos integradas que abarcan AWS servicios , software de código abierto y software COTS. Para obtener más información al respecto, consulte Fuentes de datos integradas en la documentación de Amazon Managed Grafana. También puede añadir soporte para más fuentes de datos actualizando su espacio de trabajo a Grafana Enterprise. Grafana también admite complementos de fuentes de datos que le permiten comunicarse con diferentes

	sistemas externos. CloudWatch Los paneles requieren una CloudWatch métrica o una consulta de CloudWatch Logs Insights para que los datos se muestren en un CloudWatch panel.
Gestione el acceso a su solución de paneles de forma independiente del acceso a su cuenta AWS	Amazon Managed Grafana requiere el uso de AWS IAM Identity Center (IAM Identity Center) y AWS Organizations para la autenticación y la autorización. Esto le permite autenticar a los usuarios en Grafana mediante una federació n de identidades que quizás ya utilice con IAM Identity Center o. AWS Organizations Sin embargo, si no utilizas el Centro de Identidad de IAM o AWS Organizations, entonces se configura como parte del proceso de configura ción de Grafana gestionado por Amazon. Esto podría convertirse en un problema si su organización ha limitado el uso del Centro de Identidad de IAM o. AWS Organizations

Incorpore y acceda a los datos de varias cuentas y regiones mediante la integración AWS Organizations	Amazon Managed Grafana se integra AWS Organizations para que puedas leer datos de AWS fuentes como CloudWatch Amazon OpenSearch Service en todas tus cuentas. Esto permite crear paneles de control que muestren visualizaciones utilizando los datos de sus cuentas. Para habilitar automáticamente el acceso a los datos en todas partes AWS Organizations, debes configurar tu espacio de trabajo de Grafana gestionado por Amazon en la cuenta AWS Organizations de administr ación. Esto no se recomienda según las prácticas AWS Organizations recomenda das para la cuenta de administración. Por el contrario, CloudWatch también admite paneles de control multicuentas y regiones para las métricas. CloudWatch
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 utilizar al crear sus cuadros de mando. También hay una gran biblioteca de paneles aportados por la comunidad que puede editar y reutilizar según sus necesidades.
Utilice paneles con despliegues de Grafana nuevos y existentes	Si ya utilizas Grafana, puedes importar y exportar cuadros de mando desde tus despliegues de Grafana y personalizarlos para usarlos en Amazon Managed Grafana. Amazon Managed Grafana le permite estandarizar Grafana como solución de dashboards.

Instalación y configuración avanzadas de 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 ayudarle a cumplir requisitos de casos de uso más avanzados, así como configuraciones de seguridad avanzadas. Las capacidades avanzadas pueden requerir que tus equipos aumenten su experiencia con Grafana si aún no tienen estas habilidades.

Diseño e implementación del registro y la supervisión con CloudWatch preguntas frecuentes

Esta sección proporciona respuestas a las preguntas más frecuentes sobre el diseño e implementación de una solución de registro y monitoreo con CloudWatch.

¿Dónde guardo mis archivos CloudWatch de configuración?

El CloudWatch agente para Amazon EC2 puede aplicar varios archivos de configuración que se almacenan en el directorio de CloudWatch configuración. Lo ideal es almacenar la CloudWatch configuración como un conjunto de archivos, ya que puede controlar las versiones y volver a utilizarlos en varias cuentas y entornos. Para obtener más información al respecto, consulte la Administrar CloudWatch las configuraciones sección de esta guía. Como alternativa, puede almacenar los archivos de configuración en un repositorio GitHub y automatizar la recuperación de los archivos de configuración cuando se aprovisione una nueva instancia de EC2.

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

El sistema de gestión de servicios se integra con un tema del Amazon Simple Notification Service (Amazon SNS) y se configura CloudWatch la alarma para que notifique al tema de SNS cuando se produzca una alarma. Su sistema integrado recibe el mensaje del SNS y puede crear un ticket utilizando sus sistemas de gestión de servicios o. APIs SDKs

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

Las tareas de Amazon ECS y los pods de Amazon EKS se pueden configurar para enviar automáticamente la salida de STDOUT y STDERR a. CloudWatch El enfoque recomendado para registrar las aplicaciones en contenedores es hacer que los contenedores envíen su salida a STDOUT y STDERR. Esto también se trata en el manifiesto de la aplicación Twelve-Factor.

Sin embargo, si desea enviar archivos de registro específicos, puede montar un volumen en su pod de Amazon EKS o en la definición de tareas de Amazon ECS en el que la aplicación escribirá sus

archivos de lote y utilizar un contenedor lateral para que Fluentd o Fluent Bit envíen los registros. CloudWatch CloudWatch Deberías considerar la posibilidad de vincular simbólicamente un archivo de registro específico de tu contenedor a y. `/dev/stdout` `/dev/stderr` Para obtener más información al respecto, consulta Ver los registros de un contenedor o servicio en la documentación de Docker.

¿Cómo superviso los problemas de salud de los AWS servicios?

Puede usarlo Panel de AWS Healthpara monitorear los eventos AWS de salud. También puede consultar el aws-health-tools GitHub repositorio para ver ejemplos de soluciones de automatización relacionadas con eventos de AWS salud.

¿Cómo puedo crear una CloudWatch métrica personalizada cuando no hay soporte de agentes?

Puedes usar el formato de métrica integrado para incorporar CloudWatch métricas. También puedes usar el AWS SDK (por ejemplo, put_metric_data), AWS CLI (por ejemplo, put-metric-data) o la AWS API (por ejemplo, PutMetricData) para crear métricas personalizadas. Deberías tener en cuenta cómo se mantendrá cualquier lógica personalizada a largo plazo. Un enfoque sería utilizar Lambda con soporte de formato métrico integrado para crear las métricas, junto con una regla de programación de CloudWatch eventos de eventos para establecer el período de la métrica.

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

Debe consultar las instrucciones proporcionadas por el proveedor del software o servicio para realizar la integración con ellas AWS. Es posible que puedas usar el software del agente, el SDK o una API proporcionada para enviar los registros y las métricas a su solución. También puedes usar una solución de código abierto, como Fluentd o Fluent Bit, configurada según las especificaciones del proveedor. También puede usar los filtros de suscripción de AWS SDK y CloudWatch Logs con Lambda y Kinesis Data Streams para crear procesadores de registros y remitentes personalizados. Por último, también debe tener en cuenta cómo va a integrar el software si utiliza varias cuentas y regiones.

Recursos

Introducción

- AWS Well-Architected

Resultados empresariales específicos

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

Planificar su CloudWatch despliegue

- Terminología y conceptos de AWS Organizations
- AWS Systems Manager Configuración rápida
- Recopilación de métricas y registros de instancias de Amazon EC2 y servidores locales con el agente CloudWatch
- cloudwatch-config-s.yaml de 3 cubos
- Cree el archivo de configuración del CloudWatch agente con el asistente
- Enterprise DevOps: ¿Por qué deberías ejecutar lo que has creado
- Exporting log data to Amazon S3
- Control de acceso detallado en Amazon Service OpenSearch
- Cuotas Lambda
- Cree o edite manualmente el archivo de configuración del CloudWatch agente
- Procesamiento en tiempo real de los datos de registro con suscripciones
- Herramientas sobre las que construir AWS

Configuración del CloudWatch agente para las instancias EC2 y los servidores locales

- Dimensiones métricas de Amazon EC2

- Instancias de rendimiento explosivo
- CloudWatch conjuntos de métricas predefinidos por el agente
- Recopile las métricas del proceso con el complemento procstat
- Configuración del CloudWatch agente para procstat
- Gestione la supervisión detallada de sus instancias EC2
- Ingiera registros de alta cardinalidad y genera métricas con un formato métrico integrado CloudWatch
- Trabajar con grupos de registros y flujos de registros
- Enumere CloudWatch las métricas disponibles para sus instancias
- PutLogEvents
- Recupera métricas personalizadas con collectd
- Recupera métricas personalizadas con StatsD

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

- Creación del rol de servicio de IAM requerido para Systems Manager en entornos híbridos y multinube
- Cree una activación de instancia administrada para un entorno híbrido
- Cree funciones y usuarios de IAM para usarlos con el agente CloudWatch
- Descargue y configure el CloudWatch agente mediante 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 de conjuntos de pilas
- Uso de instancias puntuales

Registro y supervisión en Amazon ECS

- amazon-cloudwatch-logs-for-fluent-bit
- CloudWatchMétricas de Amazon ECS

- Métricas de Información de contenedores de Amazon ECS
- Agente de contenedores Amazon ECS
- Tipos de lanzamiento de Amazon ECS
- Implementación del CloudWatch agente para recopilar métricas a nivel de instancia de EC2 en Amazon ECS
- ecs_cluster_with_cloudwatch_linux.yaml
- ecs_cw_emf_example
- ecs_firelense_emf_example
- ecs-task-nginx-firelense.json
- Recuperación de metadatos de AMI optimizados para Amazon ECS
- Uso del controlador de registro awslogs
- Uso de las bibliotecas cliente para generar registros integrados en formato métrico

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
- Monitorización de métricas de Prometheus de Container Insights
- Métricas del plano de control con Prometheus
- Explotación forestal de Fargate
- Fluent Bit para Amazon EKS en Fargate
- Cómo capturar los registros de las aplicaciones cuando se utiliza Amazon EKS en Fargate
- Instalación del CloudWatch agente para recopilar las métricas de Prometheus
- Instalación del servidor de métricas de Kubernetes
- kubernetes /dashboard
- Escalador automático de Kubernetes Horizontal Pod
- Componentes del plano de control de Kubernetes

- Cápsulas de Kubernetes
- Soporte para plantillas de lanzamiento
- Grupos de nodos administrados
- Comportamiento de actualización de nodos gestionados
- servidor de métricas
- Supervisión de Amazon EKS en Fargate con Prometheus y Grafana
- prometheus_jmx
- prometheus//jmx_exporter
- Extraer fuentes adicionales de Prometheus e importar esas métricas
- Nodos autoadministrados
- Envía registros a Logs CloudWatch
- Configura FluentD como para enviar registros DaemonSet a Logs CloudWatch
- Configurar una carga de trabajo Java/JMX de muestra en Amazon EKS y Kubernetes
- Tutorial para añadir un nuevo objetivo de raspado de Prometheus: métricas del servidor API de Prometheus
- Escalador automático Vertical Pod

Registro y métricas para AWS Lambda

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

Búsqueda y análisis de los registros CloudWatch

- La familia Beats
- Elastic Logstash
- Elastic Stack
- Transmisión de datos de CloudWatch registros a Amazon OpenSearch Service

Opciones alarmantes con CloudWatch

- amazon-cloudwatch-auto-alarms
- AWS Conector de gestión de servicios para Jira Service Management Cloud
- AWS Conector de gestión de servicios para el centro de datos de gestión de servicios de Jira
- AWS Conector de gestión de servicios para ServiceNow

Supervisión de la disponibilidad de las aplicaciones y los servicios

- Configuración de la recuperación ante errores a nivel de DNS

Rastreo de aplicaciones con AWS X-Ray

- Red de tareas de 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 rastreo a X-Ray
- Gráfico de servicio en X-Ray

Cuadros de mando y visualizaciones con CloudWatch

- Amazon CloudWatch Metric Math simplifica la supervisión casi en tiempo real de los sistemas de archivos de Amazon EFS
- Configuración de CloudWatch Container Insights
- Uso de la matemática métrica

CloudWatch integración con AWS los servicios

- AWS CloudTrail servicios e integraciones compatibles
- Eventos Servicios de AWS de Amazon EventBridge
- Eventos de servicio de AWS ofrecidos a través de AWS CloudTrail

- Supervisión de los archivos de CloudTrail registro con CloudWatch Logs
- Publicar registros de bases de datos en CloudWatch registros
- Publicar registros de flujo en CloudWatch registros

Amazon Managed Grafana para la creación de paneles y la visualización

- Prácticas recomendadas para la cuenta de administración en AWS Organizations
- Fuentes de datos integradas para Amazon Managed Grafana
- Paneles de mando multicuentas y regiones en CloudWatch
- Plugins de Grafana

Historial de documentos

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

Cambio	Descripción	Fecha
Información de registro actualizada	Se actualizó la sección sobre el registro de AWS 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 las métricas de las aplicaciones personalizadas en la sección Metrics for Amazon ECS.	31 de enero de 2023
Se eliminaron los avisos de vista	Grafana gestionada por Amazon está disponible de forma general.	25 de mayo de 2022
Sección eliminada	CloudWatch Ya no se admite SDK Metrics.	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 la Guía AWS prescriptiva. 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: Migrar 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: Migrar la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la nube de Nube de AWS.
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: Migrar 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: Migrar la base de datos de Oracle en las instalaciones a Oracle en una instancia de EC2 en la Nube de AWS.
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma en las instalaciones a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

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

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios administrados.

ACID

Consulte atomicidad, consistencia, aislamiento, 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 una 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 de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función de agregación

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

IA

Consulte inteligencia artificial.

AIOps

Consulte 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

Enfoque de seguridad que permite usar de manera exclusiva 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 AIOps se utiliza en la estrategia de AWS migración, 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

bot malicioso

Bot destinado a causar interrupciones o daños a personas u organizaciones.

BCP

Consulte 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. Consulte también endianidad.

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

Estrategia de implementación 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 se ejecuta en el otro entorno (verde). Esta estrategia lo ayuda a hacer reversiones rápidas con un impacto mínimo.

bot

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 la información de Internet. Otros bots, conocidos como bots maliciosos, tienen como objetivo causar interrupciones o daños a personas u organizaciones.

botnet

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

branch

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 de emergencia

En circunstancias excepcionales y mediante un proceso aprobado, es una forma rápida de que un usuario pueda acceder a un Cuenta de AWS sitio al que normalmente no tiene permisos de acceso. Para más información, consulte el indicador Implement break-glass procedures en la guía de AWS Well-Architected.

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 AWS Cloud Adoption Framework.

implementación canario

Lanzamiento lento e incremental de una versión para los usuarios finales. Cuando tenga mayor confianza en la nueva versión, la implementa y reemplaza la versión actual en su totalidad.

CCoE

Consulte Centro de excelencia en la nube.

CDC

Consulte 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

Introducción intencionada de 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 integración continua y 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 CCo E en el blog de estrategia Nube de AWS empresarial.

computación en la nube

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

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 siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCo E, 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 en el blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte base de datos de administración de 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. Algunos repositorios en la nube comunes son GitHub o Bitbucket Cloud. 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 machine learning para analizar y extraer información de formatos visuales, como imágenes y videos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

deriva de configuración

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

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

Un conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus controles 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, puesta en escena y producción del proceso de publicación del software. CI/CD se describe comúnmente como una canalización. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar más rápido. 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.

deriva 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 deriva de 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

Marco de arquitectura que proporciona una propiedad de datos distribuida y descentralizada con una administración y una gobernanza centralizadas.

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

Sistema de administración de datos que respalda la inteligencia empresarial, como los análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para las consultas y los 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 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 en 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 suelen utilizar para restringir consultas, filtrarlas y etiquetar los 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)

Estrategia y proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos a causa de 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 lenguaje de manipulación de bases de datos.

diseño basado en el dominio

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

DR

Consulte recuperación ante desastres.

Detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración con línea de base. 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 asignación de flujos de valor para el desarrollo.

E

EDA

Consulte análisis de datos de tipo exploratorio.

EDI

Consulte intercambio electrónico 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 la nube, la computación de periferia puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

Intercambio automatizado de documentos comerciales entre organizaciones. Para más información, consulte ¿Qué es el intercambio electrónico de datos?

cifrado

Proceso de computación que transforma datos de texto plano, que son 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 punto de conexión de 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 Cuentas de AWS o a responsables AWS Identity and Access Management (de 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)

Sistema que automatiza y administra los procesos empresariales clave (como la contabilidad, MES y la administración 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).

entorno

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 un CI/CD proceso, 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.

ERP

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 hechos

Tabla central de un esquema en estrella. Almacena datos cuantitativos sobre operaciones empresariales. Por lo general, 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.

Fail Fast

Filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de los enfoques ágiles.

límite de aislamiento de errores

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 más información, consulte AWS Fault Isolation Boundaries.

rama de característica

Consulte rama.

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.

peticiones con pocos pasos

Proporcionar a un LLM una pequeña cantidad de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que lleve a cabo una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, mediante el que los modelos aprenden a partir de ejemplos (pasos) incrustados en las peticiones. La técnica de peticiones con pocos pasos puede ser eficaz para las tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también peticiones desde cero.

FGAC

Consulte 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 de cambio 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.

FM

Consulte modelo fundacional.

Modelo fundacional (FM)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar una

amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para más información, consulte ¿Qué son los modelos fundacionales?

G

IA generativa

Subconjunto de modelos de IA que se entrenaron con grandes cantidades de datos y que pueden utilizar una simple petición de texto para crear contenido y artefactos nuevos, como imágenes, videos, texto y audio. Para más información, consulte ¿Qué es la IA generativa?

bloqueo geográfico

Consulte 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 la sección 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, mientras que el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

imagen dorada

Instantánea de un sistema o software que se usa como plantilla para implementar nuevas instancias de ese sistema o software. Por ejemplo, en la fabricación, una imagen dorada se puede utilizar para aprovisionar software en varios dispositivos y ayuda a mejorar la velocidad, la escalabilidad y la productividad de las operaciones de fabricación de dispositivos.

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 el cumplimiento en todas las unidades organizativas (OUs). 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 CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

HA

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.

datos de reserva

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de machine learning. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo mediante la comparación de las predicciones del modelo con los datos de reserva.

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, una revisión suele realizarse fuera del flujo de trabajo de DevOps publicación típico.

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

Consulte infraestructura como código.

políticas basadas en identidades

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

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

Modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar o modificar la infraestructura existente o aplicarle revisiones. Las infraestructuras inmutables son de manera intrínseca más coherentes, fiables y predecibles que las infraestructuras mutables. Para más información, consulte la práctica recomendada Implementación mediante una infraestructura inmutable en el Marco de AWS Well-Architected.

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 AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

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

Término que introdujo Klaus Schwab en 2016 para referirse a la modernización de los procesos de fabricación mediante los avances en la conectividad, los datos en tiempo real, la automatización, el análisis, la IA y el ML.

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 (T) IIo

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 de la Internet de las cosas (IIoT) industrial.

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red VPCs entre Internet y las redes locales (en una misma o Regiones de AWS diferente). La arquitectura AWS de referencia de seguridad recomienda configurar su cuenta de red con entrada, salida e inspección VPCs para proteger la interfaz bidireccional entre la 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 obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático 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 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.

modelo de lenguaje de gran tamaño (LLM)

Modelo de IA de aprendizaje profundo que se entrenó previamente con una gran cantidad de datos. Un LLM puede llevar a cabo varias tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para obtener más información, consulte Qué son. LLMs

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

Consulte Las 7 R.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Consulte también endianidad.

LLM

Consulte modelo de lenguaje de gran tamaño.

entornos inferiores

Consulte 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

Consulte rama.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware podría interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso

no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los registradores de pulsaciones de teclas.

Servicios administrados

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

sistema de ejecución de fabricación (MES)

Sistema de software para seguir, supervisar, documentar y controlar los procesos de producción que convierten las materias primas en productos acabados en la zona de producción.

MAP

Consulte Programa de aceleración de la migración.

mecanismo

Proceso completo mediante el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para hacer ajustes. Un mecanismo es un ciclo que se refuerza y mejora por 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 sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (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 una red bien definida APIs 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 AWS servicios sin servidor.

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 un uso ligero. APIs 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)

Herramienta en línea que proporciona información a fin de validar los argumentos comerciales necesarios para migrar a la Nube de AWS. La MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores de los socios 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

Enfoque utilizado para migrar una carga de trabajo a la Nube de AWS. Para más información, consulte la entrada Las 7 R de este glosario y también Mobilize your organization to accelerate large-scale migrations.

ML

Consulte machine learning.

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 más información, consulte Strategy for modernizing applications in the 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 más información, consulte Evaluating modernization readiness for applications in the 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.

MPA

Consulte Migration Portfolio Assessment.

MQTT

Consulte Message Queuing Telemetry Transport.

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

Modelo que actualiza y modifica la infraestructura actual 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 control de acceso de origen.

OAI

Consulte identidad de acceso de origen.

OCM

Consulte administración 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

Consulte acuerdo de 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.

Open Process Communications: arquitectura unificada (OPC-UA)

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

Lista de comprobación de preguntas y prácticas recomendadas asociadas que son útiles para comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles errores. Para más información, consulte Operational Readiness Reviews (ORR) en el Marco de AWS Well-Architected.

tecnología operativa (TO)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En el sector de la fabricación, 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 y AWS CloudTrail que registra todos los eventos para todos los miembros Cuentas de AWS de una organización. AWS Organizations Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte Crear un registro para una organización en la CloudTrail documentación.

administración del cambio organizacional (OCM)

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

control de acceso de origen (OAC)

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

identidad de acceso de origen (OAI)

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

ORR

Consulte revisión de la preparación operativa.

OT

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 AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la 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 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 administración del ciclo de vida del producto.

policy

Objeto que puede definir permisos (consulte política basada en identidad), especificar las condiciones de acceso (consulte política basada en recursos) o definir los permisos máximos para todas las cuentas de una organización de AWS Organizations (consulte política de control de servicio).

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.

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

Condición de consulta que devuelve `true` o `false`. En general, se encuentra en una cláusula `WHERE`.

inserción de predicados

Técnica de optimización de consultas en bases de datos que filtra los datos de la consulta antes de transferirlos. Esta técnica reduce la cantidad de datos de la base de datos relacional que se tienen que recuperar y procesar. Además, 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

Enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de desarrollo.

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o más VPCs. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Control de seguridad que se diseñó para evitar la implementación de recursos que no cumplan con la normativa. Estos controles analizan los recursos antes de aprovisionarlos. Si el recurso no cumple con los requisitos del control, no se aprovisiona. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en la sección Implementación de controles de seguridad en AWS.

administración del ciclo de vida del producto (PLM)

Administración 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 la reducción de su uso y su retirada.

entorno de producción

Consulte entorno.

controlador lógico programable (PLC)

En el sector de la fabricación, computadora adaptable y altamente fiable que supervisa las máquinas y automatiza los procesos de fabricación.

encadenamiento de peticiones

Uso de la salida de una petición de LLM como entrada para la siguiente petición a fin de generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en tareas secundarias o para refinar o ampliar de forma iterativa una respuesta preliminar. Ayuda a mejorar la precisión y la relevancia de las respuestas de un modelo y permite obtener resultados más detallados y personalizados.

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.

publish/subscribe (pub/sub)

Patrón que permite establecer 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 pueden suscribir otros microservicios. El sistema puede agregar 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

Consulte responsable, fiable, consultada e informada (RACI).

RAG

Consulte generación aumentada por recuperación.

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

Consulte responsable, fiable, consultada e informada (RACI).

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

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

Consulte Las 7 R.

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

Consulte Las 7 R.

Region

Conjunto de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para más información, consulte Specify which Regiones de AWS your account can use.

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 Las 7 R.

versión

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

reubicar

Consulte Las 7 R.

redefinir la plataforma

Consulte Las 7 R.

recomprar

Consulte Las 7 R.

resiliencia

Capacidad de una aplicación para resistir interrupciones o recuperarse de ellas. Al planificar la resiliencia en la Nube de AWS, la alta disponibilidad y la recuperación ante desastres son consideraciones comunes. Para más información, consulte Resiliencia en la Nube de AWS.

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 Las 7 R.

retirar

Consulte Las 7 R.

Generación aumentada de recuperación (RAG)

Tecnología de IA generativa mediante la que un LLM hace referencia a un origen de datos autorizado que se encuentra fuera de sus orígenes de datos de entrenamiento antes de generar una respuesta. Por ejemplo, un modelo de RAG podría hacer una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para más información, consulte ¿Qué es RAG (generación aumentada por recuperación)?

rotación

Proceso mediante el que periódicamente se actualiza un secreto para que resulte más difícil que un atacante pueda acceder 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 objetivo de punto de recuperación.

RTO

Consulte 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 Consola de administración de AWS 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 control de supervisión y adquisición de datos.

SCP

Consulte política de control de servicio.

secreta

En AWS Secrets Manager, información confidencial o restringida, como una contraseña o credenciales de usuario, que se almacena de forma cifrada. Se compone del valor del secreto y de sus metadatos. El valor del secreto puede ser binario, una sola cadena o varias cadenas. Para más información, consulte What's in a Secrets Manager secret? en la documentación de Secrets Manager.

seguridad desde el diseño

Enfoque de ingeniería de sistemas que tiene en cuenta la seguridad durante todo el proceso de desarrollo.

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 de controles de seguridad principales: preventivos, de detección, de respuesta y proactivos.

refuerzo de la seguridad

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

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

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

automatización de la respuesta de seguridad

Acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o corregirlo. Estas automatizaciones sirven como controles de seguridad preventivos o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. La modificación de un grupo de seguridad de VPC, la aplicación de revisiones a una instancia de Amazon EC2 o la rotación de credenciales son algunos ejemplos de acciones de respuesta automatizadas.

cifrado del servidor

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

política de control de servicio (SCP)

Política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPs defina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están 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)

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 con AWS la que compartes la seguridad y 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 sistema de administración de eventos e información de seguridad.

único punto de error (SPOF)

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

SLA

Consulte acuerdo de nivel de servicio.

SLI

Consulte indicador de nivel de servicio.

SLO

Consulte 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 más información, consulte Phased approach to modernizing applications in the Nube de AWS.

SPOF

Consulte único punto de error.

esquema en estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos de gran tamaño para almacenar datos transaccionales o medidos y una o varias tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para utilizarse 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.

control de supervisión y adquisición de datos (SCADA)

En el sector de la fabricación, sistema que utiliza hardware y software para supervisar 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

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

petición del sistema

Técnica para proporcionar contexto, instrucciones o pautas a un LLM para dirigir su comportamiento. Las peticiones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

T

etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudar a administrar, identificar, organizar, buscar y filtrar recursos de . 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

Un centro de tránsito de red que puede usar para interconectar sus redes con VPCs las locales. 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

Consulte 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

Una conexión entre dos VPCs que le 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 hace un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para las tareas de procesamiento, 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.

WORM

Consulte escritura única y lectura múltiple.

WQF

Consulte AWS Workload Qualification Framework.

escritura única y lectura múltiple (WORM)

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

Z

ataque de día cero

Ataque, normalmente de malware, que se aprovecha de 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.

peticiones desde cero

Proporcionar a un LLM instrucciones para llevar a cabo una tarea, pero sin ejemplos (pasos) que puedan ayudar a guiarlo. El LLM debe usar los conocimientos del entrenamiento previo para llevar a cabo la tarea. La eficacia de la petición desde cero depende de la complejidad de la tarea y de la calidad de la petición. Consulte también peticiones con pocos pasos.

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.