aws

Herramientas y prácticas recomendadas de supervisión y alertas para Amazon RDS para MySQL y MariaDB

AWS Guía prescriptiva

AWS Guía prescriptiva: Herramientas y prácticas recomendadas de supervisión y alertas para Amazon RDS para MySQL y MariaDB

Table of Contents

Herramientas y prácticas recomendadas de supervisión y alertas para Amazon RDS para MySQL y MariaDB

Igor Obradovic, Amazon Web Services (AWS)

Marzo de 2025 (historia del documento)

La supervisión de bases de datos es el proceso de medir, seguir y evaluar la disponibilidad, el rendimiento y la funcionalidad de una base de datos. Las soluciones de supervisión y alertas ayudan a las organizaciones a garantizar que sus servicios de bases de datos y, por lo tanto, sus aplicaciones y cargas de trabajo asociadas, sean seguros, de alto rendimiento, resistentes y eficientes. También AWS puede recopilar y analizar los registros, métricas, eventos y rastreos de su carga de trabajo para comprender el estado de su carga de trabajo y obtener información sobre las operaciones a lo largo del tiempo.

Puede supervisar los recursos para asegurarse de que funcionan según lo esperado y para detectar y solucionar los problemas antes de que afecte a los clientes. Debe utilizar las métricas, los registros, los eventos y los seguimientos que supervisa para generar las alarmas cuando se superen los umbrales.

En esta guía se describen las herramientas de supervisión y observabilidad de las bases de datos y las prácticas recomendadas para las bases de datos de Amazon Relational Database Service (Amazon RDS). La guía se centra en las bases de datos de MySQL y MariaDB, aunque la mayor parte de la información también se aplica a otros motores de bases de datos de Amazon RDS.

Esta guía está dirigida a arquitectos de soluciones, arquitectos de bases de datos DBAs, DevOps ingenieros sénior y otros miembros del equipo que se dedican a diseñar, implementar y administrar soluciones de monitoreo y observabilidad para las cargas de trabajo de sus bases de datos que se ejecutan en ellas. Nube de AWS

Contenido

Descripción general

La supervisión y las alertas se incluyen en cuatro pilares del marco de AWS Well-Architected.

- El pilar de la excelencia operativa establece que la carga de trabajo debe diseñarse de manera que incluya la telemetría y la supervisión. Los productos de AWS como Amazon Relational Database Service (Amazon RDS) proporcionan la información necesaria para que pueda comprender el estado interno de la carga de trabajo (por ejemplo, métricas, registros, eventos y seguimientos). Cuando utilice las bases de datos de Amazon RDS, querrá comprender el estado de las instancias de las bases de datos, detectar eventos operativos y poder responder a eventos planificados y no planificados. AWS proporciona herramientas de supervisión que son útiles para determinar cuándo están en riesgo los resultados de la organización y el negocio o podrían estarlo, para que pueda tomar las medidas adecuadas en el momento adecuado.
- El pilar de la eficiencia del rendimiento prescribe que debe supervisar el rendimiento de los recursos, como las instancias de base de datos de Amazon RDS, mediante la recopilación, la agregación y el procesamiento de métricas relacionadas con el rendimiento en tiempo real. Puede identificar la degradación del rendimiento y corregir los factores que la provocaron (por ejemplo, consultas SQL no optimizadas o parámetros de configuración inadecuados). Puede activar las alarmas de manera automática cuando las mediciones superen los límites esperados. Le recomendamos utilizar las alarmas no solo para las notificaciones, sino también para iniciar acciones automatizadas en respuesta a los eventos detectados. Puede evaluar las métricas que recopila en función de los umbrales predefinidos o utilizar algoritmos de machine learning para identificar un comportamiento anómalo. Por ejemplo, para detectar una tendencia del aumento del uso de la CPU, puede recopilar y analizar la métrica `cpuUtilization.total` durante un periodo. Alertar sobre esa anomalía de manera proactiva, antes de que el uso de la CPU alcance el límite máximo, puede ser útil para solucionar el problema antes de que afecte a los clientes.
- El pilar de fiabilidad define la supervisión y las alertas como indispensables para garantizar el cumplimiento de los requisitos de disponibilidad. La solución de supervisión debe poder detectar los errores de manera eficaz. Cuando detecta problemas o errores, su objetivo principal es alertar sobre esos problemas. La implementación de prácticas continuas de observabilidad y supervisión es imprescindible para las arquitecturas resilientes en la nube. Para mejorar las cargas de trabajo, debe poder medirlas y comprender su estado e integridad. Los principios de diseño para la recuperación automática en caso de error, la escalabilidad horizontal y el aprovisionamiento de capacidad dependen de la precisión de los servicios de supervisión y alerta.

- El pilar de seguridad analiza la detección y prevención de los cambios de configuración inesperados o no deseados y los comportamientos inesperados. Puede configurar las instancias de base de datos de Amazon RDS para MySQL y MariaDB con el complemento de auditoría de MariaDB para registrar la actividad de la base de datos, como los inicios de sesión de los usuarios y las operaciones concretas que se ejecutan en la base de datos. El complemento almacena el registro de la actividad de la base de datos en un archivo de registro, que se puede integrar e importar a las herramientas de supervisión y alerta. El archivo de registro se analiza en tiempo real para detectar los comportamientos inesperados o sospechosos en la base de datos. Este comportamiento inesperado o sospechoso puede indicar que la instancia de base de datos de Amazon RDS se vio comprometida, lo que indica posibles riesgos para su empresa. Si la herramienta de supervisión detecta un evento de este tipo, activa una alarma para iniciar una respuesta al incidente de seguridad, lo que ayuda a abordar las actividades sospechosas y maliciosas.

Resultados empresariales específicos

La implementación de prácticas recomendadas en los mecanismos de supervisión y alerta ayuda a garantizar una infraestructura de alto rendimiento, resistente, eficiente, segura y con optimización de costos para las aplicaciones y cargas de trabajo. Puede utilizar herramientas de observabilidad que recopilan, almacenan y visualizan métricas, eventos, seguimientos y registros en tiempo real para observar y analizar el panorama general del estado y el rendimiento de las bases de datos y, de este modo, evitar la degradación o la interrupción de los servicios de TI asociados. Si sigue produciéndose una degradación imprevista o una interrupción del servicio, las herramientas de supervisión y alerta ayudan a detectar el problema a tiempo, a escalarlo y a reaccionar, así como a investigar y resolver con rapidez. Una solución integral de supervisión y alertas para las cargas de trabajo de bases de datos en la nube ayuda a lograr los siguientes resultados empresariales:

- Mejore la experiencia del cliente. Un servicio fiable mejora la experiencia de los clientes. Las bases de datos suelen ser un componente clave de los servicios digitales, como las aplicaciones web y móviles, la transmisión de contenido multimedia, los pagos, las API de empresa a empresa (B2B) y los servicios de integración. Si puede supervisar y configurar alertas en las bases de datos para detectar los problemas de manera rápida, investigarlos de manera eficiente y solucionarlos lo antes posible para minimizar el tiempo de inactividad y otras interrupciones, puede mejorar la disponibilidad, la seguridad y el rendimiento del servicio digital para los clientes.
- Genere confianza en los clientes.Un mejor rendimiento y una experiencia de usuario más fluida le son útiles para ganarse la confianza de los clientes, lo que puede traducirse en más negocios

en su plataforma. Por ejemplo, un proveedor de servicios de procesamiento de pagos que ofrece un servicio confiable por internet puede esperar que los clientes confíen y tengan lealtad en gran medida, lo que se traduce en más clientes y una mejor retención, un aumento de las transacciones facturables y servicios nuevos e innovadores que generan más ingresos.

- Evite las pérdidas financieras.Los tiempos de inactividad inesperados en la infraestructura de la base de datos pueden afectar a las transacciones comerciales que hacen los clientes con la aplicación. En algunos casos, esto puede provocar pérdidas financieras sustanciales. El incumplimiento de los acuerdos de nivel de servicio (SLA) puede provocar que los clientes pierdan la confianza y, en consecuencia, pierda ingresos. También puede convertirse en una base legal para juicios costosos, en los que los clientes pueden exigir una compensación según los contratos de responsabilidad y garantía. Según un estudio de Atlassian Corporation, una empresa de software, los costos promedio de una interrupción del servicio oscilan entre 140 000 USD y 540 000 USD por hora, según el tipo y el tamaño de la empresa. Un entorno de base de datos estable es clave para evitar interrupciones prolongadas y pérdidas comerciales.
- Amplíe el valor. Los mecanismos de supervisión y alerta pueden ser útiles para diseñar, desarrollar y operar un servicio digital de alta disponibilidad, resiliente, confiable, eficiente, rentable y seguro, pero esto es solo el comienzo. Querrá que su organización escale y prospere con el tiempo, mejore las cargas de trabajo existentes en la nube e introduzca nuevos servicios. Los nuevos servicios proporcionan un valor adicional a los clientes y más ingresos a la empresa, lo que repercute en el crecimiento de la empresa.
- Mejore la productividad de los desarrolladores. Los desarrolladores productivos y eficientes, y que no encuentran problemas ni cuellos de botella en sus tareas de desarrollo, pueden ofrecer productos de alta calidad en menos tiempo. Sin embargo, la ingeniería de software y las operaciones de TI suelen enfrentarse a desafíos complejos. Esta complejidad aumenta con la escala de las cargas de trabajo y sus arquitecturas. Para analizar el rendimiento y la coherencia de las aplicaciones distribuidas, los desarrolladores necesitan herramientas que puedan proporcionar métricas y seguimientos correlacionados. Ayudan a identificar los artefactos de código y los componentes de infraestructura defectuosos lo más rápido posible, y ayudan a determinar los impactos en los usuarios finales. El conjunto adecuado de herramientas de supervisión y alerta puede ayudar a los desarrolladores a programar y probar mejor y más rápido.
- Mejore la eficacia y la eficiencia operativas.Al operar las cargas de trabajo en la nube a escala, incluso un pequeño porcentaje de las mejoras de rendimiento puede suponer un ahorro de millones de dólares. Al supervisar las bases de datos y analizar las métricas, los eventos, los registros y los seguimientos, puede comprender y predecir sus necesidades de capacidad futuras y aprovechar los ahorros de costos disponibles en la Nube de AWS. Comprender las cargas de

trabajo y el estado operativo de Amazon RDS puede ayudar a responder a los eventos, solucionar los problemas y planificar las mejoras.

Prácticas recomendadas generales

Las siguientes prácticas recomendadas son útiles para obtener una visibilidad suficiente del estado de la carga de trabajo de Amazon RDS y a tomar las medidas adecuadas en respuesta a los eventos operativos y los datos de supervisión.

- Identifique los KPI. Identifique los indicadores clave de rendimiento (KPI) según los resultados empresariales deseados. Evalúe los KPI para determinar los buenos resultados de la carga de trabajo. Por ejemplo, si su actividad principal es el comercio electrónico, uno de los resultados empresariales esperados podría ser que su tienda electrónica esté disponible de manera ininterrumpida para que sus clientes puedan comprar. Para lograr ese resultado empresarial, debe definir el KPI de disponibilidad para la base de datos backend de Amazon RDS que utiliza la aplicación de su tienda electrónica y establecer el KPI de la línea de base en el 99,99 % semanalmente. La evaluación del KPI de disponibilidad real con respecto al valor de la línea de base es útil para determinar si cumple con la disponibilidad deseada de la base de datos del 99,99 % y, por lo tanto, a lograr el resultado empresarial de contar con un servicio ininterrumpido.
- Defina las métricas de carga de trabajo. Defina las métricas de carga de trabajo para medir las cantidades y calidades de la carga de trabajo de Amazon RDS. Evalúe las métricas para determinar si la carga de trabajo está logrando los resultados deseados y para comprender su estado. Por ejemplo, para evaluar el KPI de disponibilidad de la instancia de bases de datos de Amazon RDS, debe medir métricas como el tiempo de actividad y el tiempo de inactividad de la instancia de bases de datos. A continuación, puede utilizar esas métricas para calcular el KPI de disponibilidad de la siguiente manera:

  ```
  availability = uptime / (uptime + downtime)
  ```

  Las métricas representan conjuntos de puntos de datos ordenados por tiempo. Las métricas también pueden incluir dimensiones. Estas son útiles en la categorización y el análisis.
- Recopile y analice las métricas de la carga de trabajo. Amazon RDS genera diferentes métricas y registros según la configuración. Algunos de estos representan eventos de instancias de bases de datos, contadores o estadísticas, como `db.Cache.innoDB_buffer_pool_hits`. Otras métricas provienen del sistema operativo, por ejemplo `memory.Total`, que mide la cantidad total de memoria de la instancia de Amazon Elastic Compute Cloud (Amazon EC2) del host. La herramienta de supervisión debe hacer un análisis periódico y proactivo de las métricas recopiladas para identificar las tendencias y determinar si se necesitan respuestas adecuadas.

- Establezca líneas de base para las métricas de carga de trabajo. Establezca las líneas de base para las métricas a fin de definir los valores esperados e identificar los umbrales correctos o incorrectos. Por ejemplo, podría definir que la línea de base para `ReadIOPS` sea de hasta 1000 en operaciones normales de base de datos. A continuación, puede utilizar esta línea de base para comparar e identificar el sobreúso. Si las nuevas métricas muestran de manera coherente que las IOPS leídas oscilan entre 2000 y 3000, habrá identificado una desviación que podría provocar una respuesta que permitiera investigar, intervenir y mejorar.
- Alerte cuando los resultados de la carga de trabajo estén en riesgo. Cuando determine que el resultado empresarial está en riesgo, emita una alerta. A continuación, puede abordar los problemas de forma proactiva, antes de que afecten a los clientes, o mitigar el impacto del incidente de manera oportuna.
- Identifique los patrones de actividad esperados para la carga de trabajo. Según las métricas de la línea de base, establezca los patrones de la actividad de la carga de trabajo para identificar comportamientos inesperados y responder con las acciones adecuadas, si es necesario. AWS proporciona herramientas de supervisión que aplican algoritmos estadísticos y de machine learning para analizar las métricas y detectar las anomalías.
- Alerte cuando se detecten anomalías de la carga de trabajo. Cuando se detecten las anomalías en las operaciones de las cargas de trabajo de Amazon RDS, emita una alerta para que pueda responder con las medidas adecuadas si es necesario.
- Evalúe y revise los KPI y las métricas. Confirme que las bases de datos de Amazon RDS cumplen los requisitos definidos e identifique las áreas de posibles mejoras para alcanzar sus objetivos empresariales. Valide la eficacia de las métricas medidas y los KPI evaluados. Revíselos si es necesario. Por ejemplo, supongamos que establece un KPI para el número óptimo de conexiones simultáneas a bases de datos y que supervisa las métricas relacionadas con las conexiones intentadas y erróneas, así como los procesos de usuarios que se crearon y están en ejecución. Es posible que tenga más conexiones a bases de datos que las definidas en la línea de base del KPI. Al analizar las métricas actuales, puede detectar el resultado, pero es posible que no pueda determinar la causa de origen. Si es así, debe revisar las métricas e incluir otras medidas de supervisión, como contadores para bloquear las tablas. Las nuevas métricas ayudarían a determinar si el aumento del número de conexiones a la base de datos se debe a bloqueos de tablas inesperados.

Herramientas de supervisión

Le recomendamos utilizar herramientas de observabilidad, supervisión y alertas para lo siguiente:

- Obtenga información sobre el rendimiento del entorno de Amazon RDS
- Detecte comportamientos inesperados y sospechosos
- Planifique la capacidad y tome decisiones fundamentadas sobre la asignación de instancias de Amazon RDS
- Analice las métricas y los registros para predecir posibles problemas de forma proactiva
- Genere alertas cuando se superen los umbrales para solucionar y resolver los problemas antes de que los usuarios se vean afectados

Puede elegir entre diferentes opciones y soluciones, tales como herramientas y servicios de supervisión y observabilidad nativos en la nube proporcionados por AWS; soluciones de software gratuitas y de código abierto; y soluciones comerciales de terceros para supervisar las instancias de bases de datos de Amazon RDS. Algunas de estas herramientas se analizan en las secciones siguientes.

Para determinar qué herramienta se adapta mejor a sus necesidades, compare las características y funcionalidades de cada herramienta con los requisitos de su organización. También le recomendamos evaluar las herramientas para determinar la facilidad de implementación, configuración e integración, las actualizaciones y el mantenimiento del software, el método de implementación (por ejemplo, con hardware o sin servidor), las licencias, el precio y otros factores que sean específicos de su organización.

Secciones

Herramientas incluidas en Amazon RDS

Amazon Relational Database Service (Amazon RDS) es un servicio de bases de datos administrado en la Nube de AWS. Debido a que Amazon RDS es un servicio administrado, lo libera de la mayoría de las tareas de administración, como las copias de seguridad de bases de datos, las instalaciones del sistema operativo (SO) y el software de bases de datos, la aplicación de revisiones del sistema operativo y el software, la configuración de alta disponibilidad, el ciclo de vida del hardware y las operaciones del centro de datos. AWS también proporciona un conjunto completo de herramientas para crear una solución de observabilidad completa para las instancias de bases de datos de Amazon RDS.

Algunas de las herramientas de supervisión están incluidas, preconfiguradas y habilitadas de manera automática en el servicio Amazon RDS. En cuanto inicie la nueva instancia de Amazon RDS, tendrá a su disposición dos herramientas automatizadas:

- El estado de la instancia de Amazon RDS proporciona detalles sobre el estado actual de la instancia de bases de datos. Por ejemplo, entre los códigos de estado se incluyen Disponible, Detenida, Creando, Haciendo copia de seguridad y Error. Puede utilizar la consola de Amazon RDS, la AWS Command Line Interface (AWS CLI) o la API de Amazon RDS para ver el estado de la instancia. Para más información, consulte Ver el estado de la instancia de bases de datos de Amazon RDS en la documentación de Amazon RDS.
- Las recomendaciones de Amazon RDS ofrecen recomendaciones automatizadas para las instancias de bases de datos, réplicas de lectura y grupos de parámetros de bases de datos. Estas recomendaciones se proporcionan tras analizar el uso de la instancia de base de datos, los datos de rendimiento y la configuración. Se ofrecen a modo de orientación. Por ejemplo, la recomendación de que la versión del motor esté desactualizada sugiere que las instancias de base de datos no ejecutan la última versión del software de base de datos y que debe actualizarla para beneficiarse de las últimas correcciones de seguridad y otras mejoras. Para más información, consulte Ver las recomendaciones de Amazon RDS en la documentación de Amazon RDS.

Espacios de nombres de CloudWatch

Amazon RDS se integra con Amazon CloudWatch. Se trata de un servicio de supervisión y alertas para los recursos y las aplicaciones de la nube que se ejecutan en AWS. Amazon RDS recopila automáticamente las métricas, los archivos de registro, los seguimientos y los eventos acerca del

funcionamiento, el uso, el rendimiento y el estado de las instancias de base de datos y los envía a CloudWatch para su almacenamiento, análisis y alertas a largo plazo.

Amazon RDS para MySQL y Amazon RDS para MariaDB publican de manera automática un conjunto predeterminado de métricas en CloudWatch en intervalos de un minuto sin costo adicional. Esas métricas se recopilan en dos espacios de nombres, que son contenedores de métricas:

- El espacio de nombres de AWS/RDS incluye métricas de instancias de base de datos. Algunos ejemplos son `BinLogDiskUsage` (la cantidad de espacio en disco que ocupan los registros binarios), `CPUUtilization` (el porcentaje de uso de la CPU), `DatabaseConnections` (el número de conexiones de red del cliente a la instancia de base de datos), etc.
- El espacio de nombres AWS/Usage incluye métricas de uso de cuenta, que se utilizan para determinar si está opera dentro de las cuotas de servicio de Amazon RDS. Entre los ejemplos se incluyen `DBInstances` (el número de instancias de base de datos en su cuenta o región de AWS), `DBSubnetGroups` (el número de grupos de subredes de bases de datos en su cuenta o región de AWS) y `ManualSnapshots` (el número de instantáneas de bases de datos creadas manualmente en su cuenta o región de AWS).

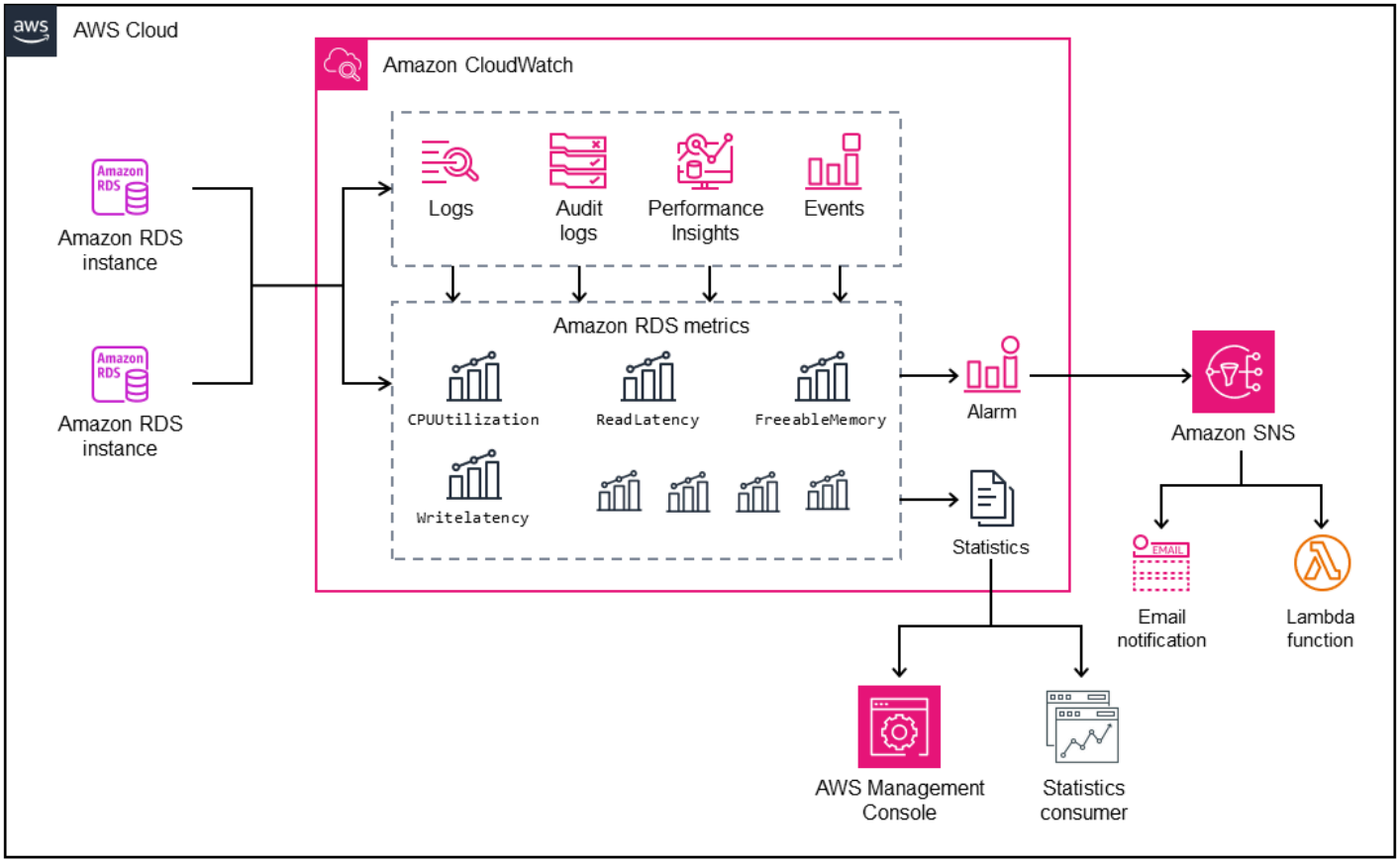
CloudWatch retiene los datos de las métricas como se indica a continuación:

- 3 horas: las métricas personalizadas de alta resolución con un periodo inferior a 60 segundos se retienen durante 3 horas. Transcurridas 3 horas, los puntos de datos se agregan en métricas de periodos de 1 minuto y se mantienen durante 15 días.
- 15 días: los puntos de datos con un periodo de 60 segundos (1 minuto) se retienen durante 15 días. Después de 15 días, los puntos de datos se agregan en métricas de periodos de 5 minutos y se conservan durante 63 días.
- 63 días: los puntos de datos con un periodo de 300 segundos (5 minutos) se retienen durante 63 días Después de 63 días, los puntos de datos se agregan en métricas de un periodo de 1 hora y se conservan durante 15 meses.
- 15 meses: los puntos de datos con un periodo de 3600 segundos (1 hora) están disponibles durante 15 meses (455 días).

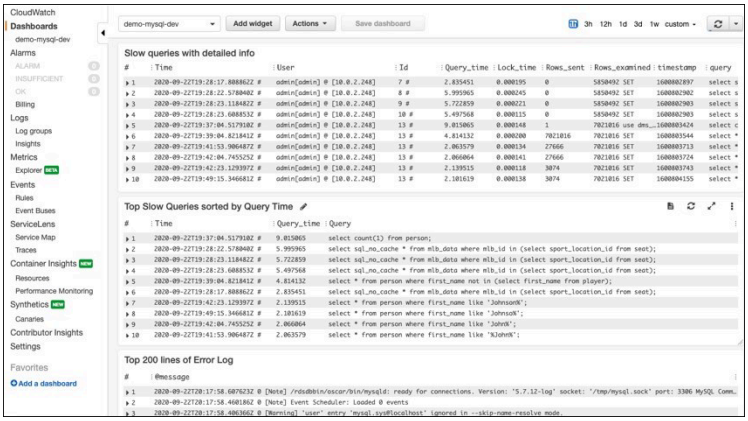
Para más información, consulte Métricas en la documentación de CloudWatch.

Alarmas y paneles de CloudWatch

Puede utilizar las alarmas de Amazon CloudWatch para supervisar una métrica específica de Amazon RDS durante un periodo. Por ejemplo, puede supervisar `FreeStorageSpace` y, a continuación, llevar a cabo una o varias acciones si el valor de la métrica supera el umbral establecido. Si establece el umbral en 250 MB y el espacio de almacenamiento libre es de 200 MB (menos que el umbral), la alarma se activará y podrá activar una acción para aprovisionar de manera automática más almacenamiento para la instancia de base de datos de Amazon RDS. La alarma también puede enviar un SMS de notificación al administrador de bases de datos mediante Amazon Simple Notification Service (Amazon SNS). En el siguiente diagrama se ilustra este proceso.

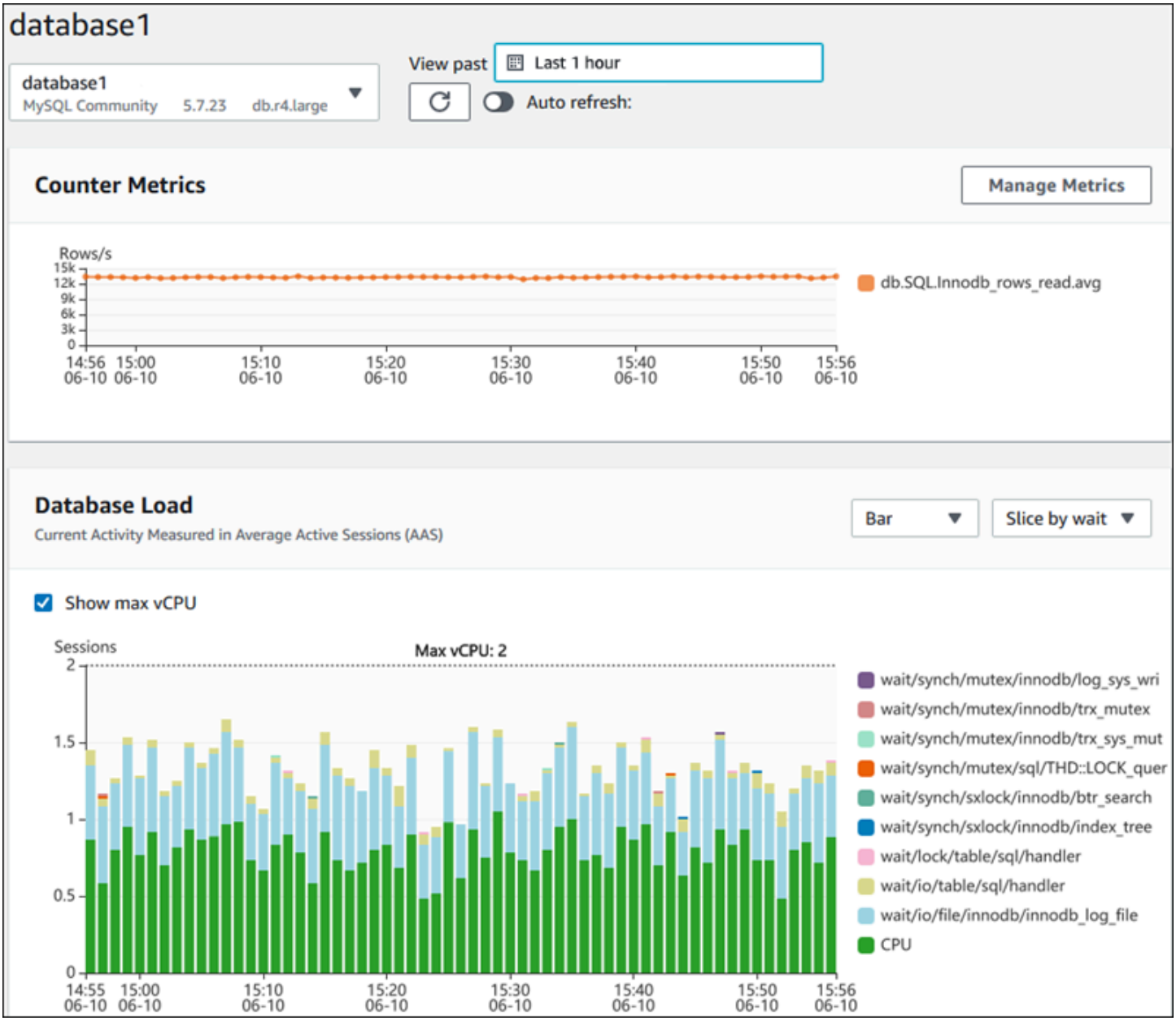


CloudWatch también proporciona paneles, que puede utilizar para crear, personalizar, interactuar y guardar vistas personalizadas (gráficos) de las métricas. También puede utilizar Información de registros de CloudWatch para crear un panel para supervisar el registro de consultas lentas y el registro de errores, así como para recibir alertas si se detecta un patrón específico en esos registros. En la pantalla siguiente, se muestra un ejemplo de un panel de CloudWatch.



Información de rendimiento de Amazon RDS

Información de rendimiento de Amazon RDS es una herramienta de ajuste y supervisión del rendimiento de la base de datos que complementa las características de supervisión de Amazon RDS. Ayuda a analizar el rendimiento de la base de datos al visualizar la carga de la instancia de base de datos y filtrarla por esperas, instrucciones SQL, hosts o usuarios. La herramienta combina varias métricas en un único gráfico interactivo que es útil para identificar el tipo de obstáculo que podría tener la instancia de base de datos, como las esperas bloqueadas, el alto consumo de CPU o la latencia de E/S. También para determinar qué instrucciones SQL generan el cuello de botella. En la pantalla siguiente, se muestra una visualización de ejemplo.



Debe habilitar Información de rendimiento durante el proceso de creación de la instancia de base de datos para recopilar las métricas de las instancias de base de datos de Amazon RDS de la cuenta. El nivel gratuito incluye siete días de historial de datos de rendimiento y un millón de solicitudes de API al mes. También puede comprar periodos de retención más largos. Para obtener información completa sobre los precios, consulte los precios de Performance Insights.

Para obtener información sobre cómo puede usar Información de rendimiento para supervisar las instancias de base de datos, consulte la sección de supervisión de instancias de base de datos más adelante en esta guía.

Información sobre rendimiento publica automáticamente las métricas en CloudWatch. Además de utilizar la herramienta Información de rendimiento, puede aprovechar las características adicionales que ofrece CloudWatch. Puede examinar las métricas de Información de rendimiento mediante la consola de CloudWatch, la AWS CLI o la API de CloudWatch. También puede agregar alarmas de CloudWatch, como con cualquier otra métrica. Por ejemplo, es posible que quiera activar una notificación por SMS a los administradores de bases de datos o tomar medidas correctivas si la métrica `DBLoad` supera el valor límite establecido. También puede agregar las métricas de Información de rendimiento a los paneles de CloudWatch existentes.

Enhanced Monitoring (Monitorización mejorada)

Enhanced Monitoring es una herramienta que captura las métricas en tiempo real para el sistema operativo (SO) en el que se ejecuta la instancia de base de datos de Amazon RDS. Estas métricas proporcionan una granularidad de hasta un segundo para la CPU, la memoria, los procesos de Amazon RDS y del sistema operativo, el sistema de archivos y los datos de E/S del disco, entre otros. Puede acceder a estas métricas y analizarlas en la consola de Amazon RDS. Al igual que con Información de rendimiento, las métricas de Enhanced Monitoring se envían de Amazon RDS a CloudWatch, donde puede beneficiarse de otras funciones, como la conservación a largo plazo de las métricas para su análisis, la creación de filtros de métricas, la visualización de gráficos en el panel de CloudWatch y la configuración de alarmas. De manera predeterminada, Enhanced Monitoring está inhabilitada al crear una nueva instancia de base de datos de Amazon RDS. Puede habilitar la característica al crear o modificar una instancia de base de datos. Los precios se basan en la cantidad de datos transferidos de Amazon RDS a Registros de CloudWatch y en las tarifas de almacenamiento. Según la granularidad y el número de instancias de base de datos en las que esté habilitada la herramienta Enhanced Monitoring, parte de los datos de supervisión se puede incluir en el nivel gratuito de Registros de CloudWatch. Para obtener los detalles de precios completos, consulte Precios de Amazon CloudWatch. Para más información sobre la herramienta, consulte la documentación de Amazon RDS y las preguntas frecuentes sobre Enhanced Monitoring.

Servicios adicionales de AWS

AWS proporciona varios servicios de apoyo, que también se integran con Amazon RDS y CloudWatch, para mejorar aún más la observabilidad de las bases de datos. Entre ellos se incluyen Amazon EventBridge, Registros de Amazon CloudWatch y AWS CloudTrail.

- Amazon EventBridge es un bus de eventos sin servidor que puede recibir, filtrar, transformar, enrutar y entregar eventos desde las aplicaciones y recursos de AWS, tales como las instancias

de base de datos de Amazon RDS. Un evento de Amazon RDS indica un cambio en el entorno de Amazon RDS. Por ejemplo, cuando una instancia de base de datos cambia su estado de Disponible a Detenida, Amazon RDS genera el evento `RDS-EVENT-0087 / The DB instance has been stopped`. Amazon RDS envía eventos a Eventos de CloudWatch y EventBridge casi en tiempo real. Con EventBridge y Eventos de CloudWatch, puede definir las reglas para enviar las alertas sobre los eventos de interés específicos de Amazon RDS y automatizar las medidas que se tomarán cuando un evento coincida con la regla. Hay una variedad de objetivos disponibles en respuesta a un evento, como una función de AWS Lambda que puede tomar una medida correctiva o un tema de Amazon SNS que puede enviar un correo electrónico o un SMS para notificar el evento a los administradores de bases de datos o ingenieros de DevOps.

- Registros de Amazon CloudWatch es un servicio que centraliza el almacenamiento de los archivos del registro de todas las aplicaciones, sistemas y productos de AWS, tales como las instancias de bases de datos de Amazon RDS para MySQL y MariaDB y AWS CloudTrail. Si habilita la característica para las instancias de base de datos, Amazon RDS publica de manera automática los registros siguientes en Registros de CloudWatch:
  - Registro de errores
  - Registro de consultas lentas
  - Registro general
  - Registro de auditoría

  Puede utilizar Información de registros de CloudWatch para consultar y analizar los datos del registro. La característica incluye un lenguaje de consulta especialmente diseñado que ayuda a consultar los eventos de registro que coincidan con los patrones que defina. Por ejemplo, puede hacer un seguimiento de los daños en las tablas de la instancia de base de datos de MySQL. Para ello, supervise el archivo del registro de errores para detectar el patrón siguiente: `"ERROR 1034 (HY000): Incorrect key file for table '*'; try to repair it OR Table * is marked as crashed"`. Los datos de registro filtrados se pueden convertir en métricas de CloudWatch. A continuación, puede utilizar las métricas para crear los paneles con los gráficos o los datos tabulares. O puede configurar una alarma si se supera el valor del umbral definido. Esto resulta muy útil cuando se utiliza el registro de auditoría, ya que puede supervisar de manera automática, enviar alertas y tomar medidas correctivas si se detectan comportamientos inesperados o sospechosos. Puede acceder a los registros de bases de datos y gestionarlos mediante la consola de administración de AWS, la AWS CLI, la API de Amazon RDS o el AWS SDK para Registros de CloudWatch.

- AWS CloudTrail registra y supervisa de manera continua la actividad de los usuarios y de las API en su Cuenta de AWS. Es útil para auditar, supervisar la seguridad y solucionar los problemas operativos de las instancias de base de datos de Amazon RDS para MySQL o MariaDB. CloudTrail se integra con Amazon RDS Todas las acciones se pueden registrar. CloudTrail proporciona un registro de las acciones de un usuario, un rol o un producto de AWS en Amazon RDS. Por ejemplo, cuando un usuario crea una nueva instancia de base de datos de Amazon RDS, se detecta un evento y el registro incluye información sobre la acción solicitada (`"eventName": "CreateDBInstance"`), la fecha y la hora de la acción (`"eventTime": "2022-07-30T22:14:06Z"`), los parámetros de la solicitud (`"requestParameters": {"dBInstanceIdentifier": "test-instance", "engine": "mysql", "dBInstanceClass": "db.m6g.large"}`), etc. Entre los eventos que registra CloudTrail se incluyen las llamadas desde la consola de Amazon RDS y las llamadas desde el código que utiliza la API de Amazon RDS.

Herramientas de supervisión de terceros

En algunos escenarios, además del conjunto completo de herramientas de supervisión y observabilidad nativas en la nube que proporciona AWS para Amazon RDS, es posible que quiera utilizar las herramientas de supervisión de otros proveedores de software. Entre estos escenarios se incluyen las implementaciones híbridas, en las que puede tener varias bases de datos ejecutándose en el centro de datos en las instalaciones y otro conjunto de bases de datos ejecutándose en la Nube de AWS. Si ya estableció su solución de observabilidad corporativa, es posible que quiera seguir utilizando las herramientas existentes y ampliarlas a sus implementaciones de Nube de AWS. El desafío de configurar una solución de supervisión de terceros suele residir en las protecciones que impone Amazon RDS como servicio administrado en la nube. Por ejemplo, no puede instalar el software de agente en el sistema operativo host que ejecuta la instancia de base de datos porque se deniega el acceso a la máquina host de la base de datos. Sin embargo, puede integrar muchas soluciones de supervisión de terceros con Amazon RDS a partir de CloudWatch y otros servicios de la Nube de AWS. Por ejemplo, las métricas, los registros, los eventos y los seguimientos de Amazon RDS se pueden exportar y, a continuación, importar a la herramienta de supervisión de terceros para su posterior análisis, visualización y alertas. Algunas de estas soluciones de terceros incluyen Prometheus, Grafana y Percona.

Prometheus y Grafana

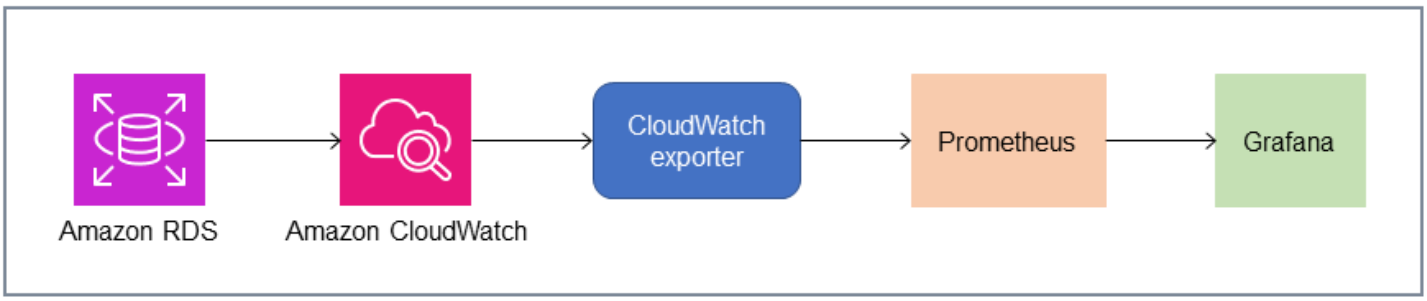
Prometheus es una solución de supervisión de código abierto que recopila las métricas de objetivos configurados a intervalos determinados. Es una solución de supervisión de uso general que puede supervisar cualquier aplicación o servicio. Cuando supervisa las instancias de base de datos de Amazon RDS, CloudWatch recopila las métricas de Amazon RDS. A continuación, las métricas se exportan al servidor de Prometheus mediante un exportador de código abierto, como el exportador YACE o CloudWatch Exporter.

- El exportador YACE optimiza las tareas de exportación de los datos al recuperar varias métricas en una sola solicitud a la API de CloudWatch. Una vez almacenadas las métricas en el servidor de Prometheus, este evalúa las expresiones de las reglas y puede generar las alertas cuando se cumplen condiciones específicas.
- Prometheus mantiene oficialmente CloudWatch Exporter. Recupera las métricas de CloudWatch a través de la API de CloudWatch y las almacena en el servidor de Prometheus en un formato compatible con Prometheus, mediante solicitudes de la API de REST al punto de conexión HTTP.

Cuando elija un exportador, diseñe su modelo de implementación y configure las instancias del exportador, tenga en cuenta las cuotas de API y servicio de CloudWatch y Registro de CloudWatch, ya que la exportación de las métricas de CloudWatch a un servidor de Prometheus se implementa sobre la API de CloudWatch. Por ejemplo, si se implementan varias instancias de CloudWatch Exporter en una sola Cuenta de AWS y región para supervisar cientos de instancias de base de datos de Amazon RDS, se podría producir un error de limitación (ThrottlingException) y errores de código 400. Para superar estas limitaciones, considere la posibilidad de utilizar el exportador YACE, que está optimizado para recopilar hasta 500 métricas diferentes en una sola solicitud. Además, para implementar un gran número de instancias de base de datos de Amazon RDS, debe considerar el uso de varias Cuentas de AWS, en lugar de centralizar la carga de trabajo en una sola Cuenta de AWS y limitar el número de instancias del exportador en cada Cuenta de AWS.

El servidor de Prometheus genera las alertas y Alertmanager las gestiona. Esta herramienta se encarga de deduplicar, agrupar y enrutar las alertas al destinatario correcto, como correo electrónico, SMS o Slack, o de iniciar una acción de respuesta automática. Otra herramienta de código abierto llamada Grafana muestra visualizaciones de estas métricas. Grafana proporciona widgets de visualización enriquecidos, como gráficos avanzados, paneles dinámicos y características de análisis, como consultas ad hoc y desglose dinámico. También puede buscar y analizar los registros,

e incluye características de alerta para evaluar de manera continua las métricas y los registros, y enviar notificaciones cuando los datos coincidan con las reglas de alerta.



Percona

Percona Monitoring and Management (PMM) es una solución de supervisión, administración y observabilidad de bases de datos gratuita y de código abierto para MySQL y MariaDB. PMM recopila miles de métricas de rendimiento de las instancias de base de datos y sus hosts. Proporciona una interfaz de usuario web para visualizar los datos en los paneles y otras características, como asesores automáticos para las evaluaciones del estado de las bases de datos. Puede utilizar PMM para supervisar Amazon RDS. Sin embargo, el cliente (agente) de PMM no está instalado en los hosts subyacentes de las instancias de base de datos de Amazon RDS porque no tiene acceso a los hosts. En su lugar, la herramienta se conecta a las instancias de base de datos de Amazon RDS, consulta las estadísticas del servidor, `INFORMATION_SCHEMA`, el esquema del sistema y Performance Schema. Utiliza la API de CloudWatch para adquirir métricas, registros, eventos y seguimientos. PMM requiere una clave de acceso de usuario de AWS Identity and Access Management (IAM) (rol de IAM) y detecta de manera automática las instancias de base de datos de Amazon RDS disponibles para su supervisión. La herramienta PMM está perfilada para la supervisión de bases de datos y recopila más métricas específicas de bases de datos que Prometheus. Para utilizar el panel de Query Analytics de PMM, debe configurar Performance Schema como origen de consultas, ya que el agente de Query Analytics no está instalado en Amazon RDS y no puede leer el registro de consultas lentas. En su lugar, consulta `performance_schema` desde las instancias de base de datos de MySQL y MariaDB directamente para obtener las métricas. Una de las características más destacadas de PMM es su capacidad para alertar y asesorar a los administradores de bases de datos sobre los problemas que la herramienta identifica en sus bases de datos. PMM ofrece conjuntos de verificaciones que pueden detectar las amenazas de seguridad más comunes, la degradación del rendimiento, la pérdida de datos y la corrupción de los datos.

Además de estas herramientas, hay varias soluciones comerciales de observabilidad y supervisión disponibles en el mercado que se pueden integrar con Amazon RDS. Algunos ejemplos son la supervisión de bases de datos de Datadog, la supervisión de Amazon RDS de Dynatrace y la supervisión de bases de datos de AppDynamics.

Supervisión de instancias de bases de datos

La instancia de base de datos es el componente básico de Amazon RDS. Es un entorno de base de datos aislado que se ejecuta en la nube. Para las bases de datos MySQL y MariaDB, la instancia de base de datos es el programa mysqld, también conocido como servidor MySQL, que incluye varios subprocesos y componentes, como el analizador SQL, el optimizador de consultas, el controlador thread/connection , las variables de sistema y estado y uno o más motores de almacenamiento conectables. Cada motor de almacenamiento está diseñado para admitir un caso de uso especializado. El motor de almacenamiento predeterminado y recomendado es InnoDB, que es un motor de base de datos relacional, transaccional y de uso general que cumple con el modelo de atomicidad, coherencia, aislamiento y durabilidad (ACID). InnoDB presenta estructuras en memoria (grupo de búferes, búfer de cambios, índice hash adaptativo, búfer de registro) y estructuras en disco (espacios de tablas, tablas, índices, registro de reversión, registro de recuperación de cambios, archivos de búfer de doble escritura). Para garantizar que la base de datos cumpla estrictamente el modelo ACID, el motor de almacenamiento de InnoDB implementa numerosas funcionalidades para proteger los datos, entre estos las transacciones, la confirmación, la reversión, la recuperación de bloqueos, el bloqueo a nivel de fila y el control de concurrencia multiversión (MVCC).

Todos estos componentes internos de una instancia de base de datos funcionan en conjunto para mantener la disponibilidad, integridad y seguridad de los datos con el nivel de rendimiento esperado y satisfactorio. Según la carga de trabajo, cada componente y característica puede exigir recursos a los subsistemas de CPU, memoria, red y almacenamiento. Cuando el aumento de la demanda de un recurso específico supera la capacidad aprovisionada o los límites del software de ese recurso (impuestos por los parámetros de configuración o por el diseño del software), la instancia de base de datos puede sufrir una degradación del rendimiento o una falta total de disponibilidad o corrupción. Por lo tanto, es fundamental medir y supervisar estos componentes internos, compararlos con los valores definidos de la línea de base y generar alertas si los valores supervisados se desvían de los valores esperados.

Como se describió anteriormente, puede utilizar otras herramientas para supervisar las instancias de MySQL y MariaDB. Le recomendamos que utilice Performance Insights y CloudWatch las herramientas de Amazon RDS para la supervisión y las alertas, ya que estas herramientas están integradas con Amazon RDS, recopilan métricas de alta resolución, presentan la información de rendimiento más reciente prácticamente en tiempo real y generan alarmas.

Sea cual sea la herramienta de supervisión que prefiera, le recomendamos que active Performance Schema en las instancias de bases de datos de MySQL y MariaDB. Performance Schema es una

característica opcional para supervisar el funcionamiento del servidor MySQL (la instancia de base de datos) a un nivel bajo y está diseñado para tener un impacto mínimo en el rendimiento general de la base de datos. Puede administrar esta característica mediante el parámetro `performance_schema`. Si bien este parámetro es opcional, debe utilizarlo para recopilar métricas de alta resolución (un segundo) por SQL, métricas de sesión activa, eventos de espera y otra información de supervisión detallada de bajo nivel, que recopila Información de rendimiento de Amazon RDS.

Secciones

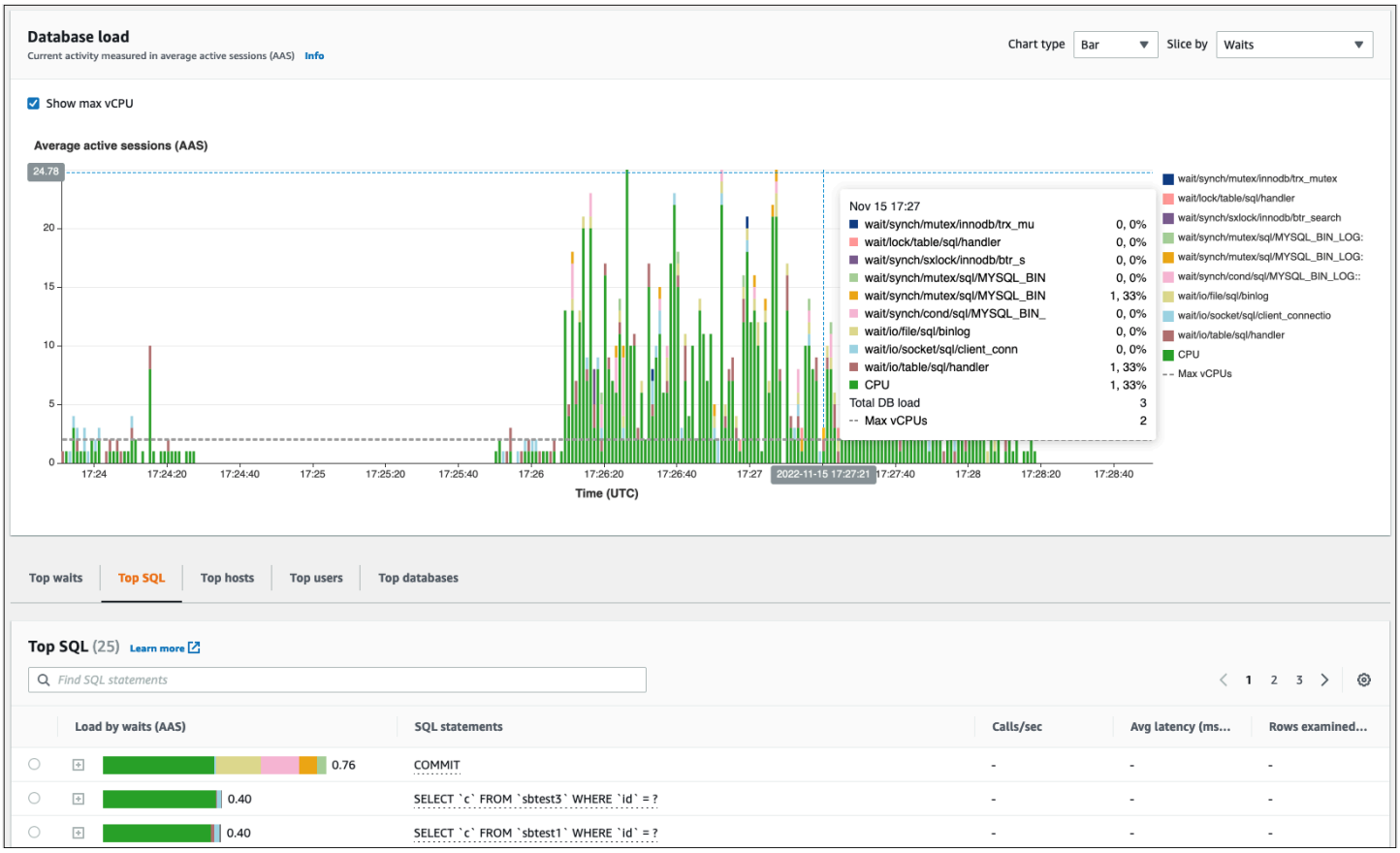
Métricas de Información de rendimiento para instancias de bases de datos

Información de rendimiento supervisa diferentes tipos de métricas, tal y como se describe en las siguientes secciones.

Carga de base de datos

La carga de la base de datos (`DBLoad`) es una métrica clave en Información de rendimiento que mide el nivel de actividad de la base de datos. Se recopila cada segundo y se publica automáticamente en Amazon CloudWatch. Representa la actividad de la instancia de base de datos en el promedio de sesiones activas (AAS), que es el número de sesiones en las que se ejecutan consultas SQL de forma simultánea. La métrica `DBLoad` es distinta de otras métricas de series temporales porque se puede interpretar mediante cualquiera de estas cinco dimensiones: esperas, SQL, hosts, usuarios y bases de datos. Estas dimensiones son subcategorías de la métrica `DBLoad`. Puede utilizarlas segmentadas por categorías para representar diferentes características de la carga de la base de datos. Para obtener una descripción detallada de cómo calculamos la carga de la base de datos, consulte Carga de la base de datos en la documentación de Amazon RDS.

La siguiente imagen muestra la herramienta Información de rendimiento.



Dimensiones

- Los eventos de espera son condiciones en las que una sesión de base de datos espera a que se complete un recurso u otra operación para continuar con su procesamiento. Si ejecuta una sentencia SQL como, `SELECT * FROM big_table` y si esta tabla es mucho más grande que el conjunto de búferes de InnoDB asignado, lo más probable es que su sesión `wait/io/file/innodb/innodb_data_file` espere a que se produzcan eventos de espera, que se deben a I/O operaciones físicas en el archivo de datos. Los eventos de espera son una dimensión importante para la supervisión de bases de datos, ya que indican posibles cuellos de botella en el rendimiento. Los eventos de espera indican a qué recursos y operaciones dedican más tiempo de espera las instrucciones SQL que ejecuta en las sesiones. Por ejemplo, el evento `wait/synch/mutex/innodb/trx_sys_mutex` se produce cuando hay una gran actividad en la base de datos con un gran número de transacciones. El evento `wait/synch/mutex/innodb/buf_pool_mutex` se produce cuando un subproceso ha adquirido un bloqueo en el grupo de búferes de InnoDB para acceder a una página en la memoria. Para más información sobre todos los eventos de espera de MariaDB y MySQL, consulte Tablas de resumen de eventos de espera en la documentación de MySQL. Para comprender cómo interpretar los nombres de los

instrumentos, consulte Convenciones de nomenclatura de instrumentos de Performance Schema en la documentación de MySQL.

- SQL muestra qué instrucciones SQL contribuyen más a la carga total de la base de datos. La tabla de dimensiones principales es interactiva. Se encuentra debajo del gráfico de la carga de la base de datos en Información de rendimiento de Amazon RDS. Puede obtener una lista detallada de los eventos de espera asociados a la instrucción SQL. Para ello, haga clic en la barra de la columna Carga por esperas (AAS). Al seleccionar una instrucción SQL de la lista, Información de rendimiento muestra los eventos de espera asociados en el diagrama de la carga de la base de datos y el texto de la instrucción SQL en la sección de texto SQL. Las estadísticas de SQL se muestran en el lado derecho de la tabla de las dimensiones principales.
- Hosts muestra los nombres de host de los clientes conectados. Esta dimensión ayuda a identificar qué hosts de los clientes envían la mayor parte de la carga a la base de datos.
- Usuarios agrupa la carga de la base de datos según los usuarios que iniciaron sesión en la base de datos.
- Bases de datos agrupa la carga de bases de datos según el nombre de la base de datos a la que está conectado el cliente.

Métricas de contador

Las métricas de contador son métricas acumulativas cuyos valores solo pueden aumentar o restablecerse a cero cuando se reinicia la instancia de base de datos. El valor de una métrica de contador no se puede reducir a su valor anterior. Estas métricas representan un contador único que aumenta de manera monótona.

- Los contadores nativos son métricas definidas por el motor de base de datos y no por Amazon RDS. Por ejemplo:
  - `SQL.Innodb_rows_inserted` representa el número de filas insertadas en las tablas de InnoDB.
  - `SQL.Select_scan` representa el número de uniones que completaron un análisis completo de la primera tabla.
  - `Cache.Innodb_buffer_pool_reads` representa el número de lecturas lógicas que el motor de InnoDB no pudo recuperar del grupo de búferes y tuvo que leer directamente del disco.
  - `Cache.Innodb_buffer_pool_read_requests` representa el número de solicitudes de lectura lógica.

Consulte las definiciones de todas las métricas nativas en Variables de estado de servidor en la documentación de MySQL.

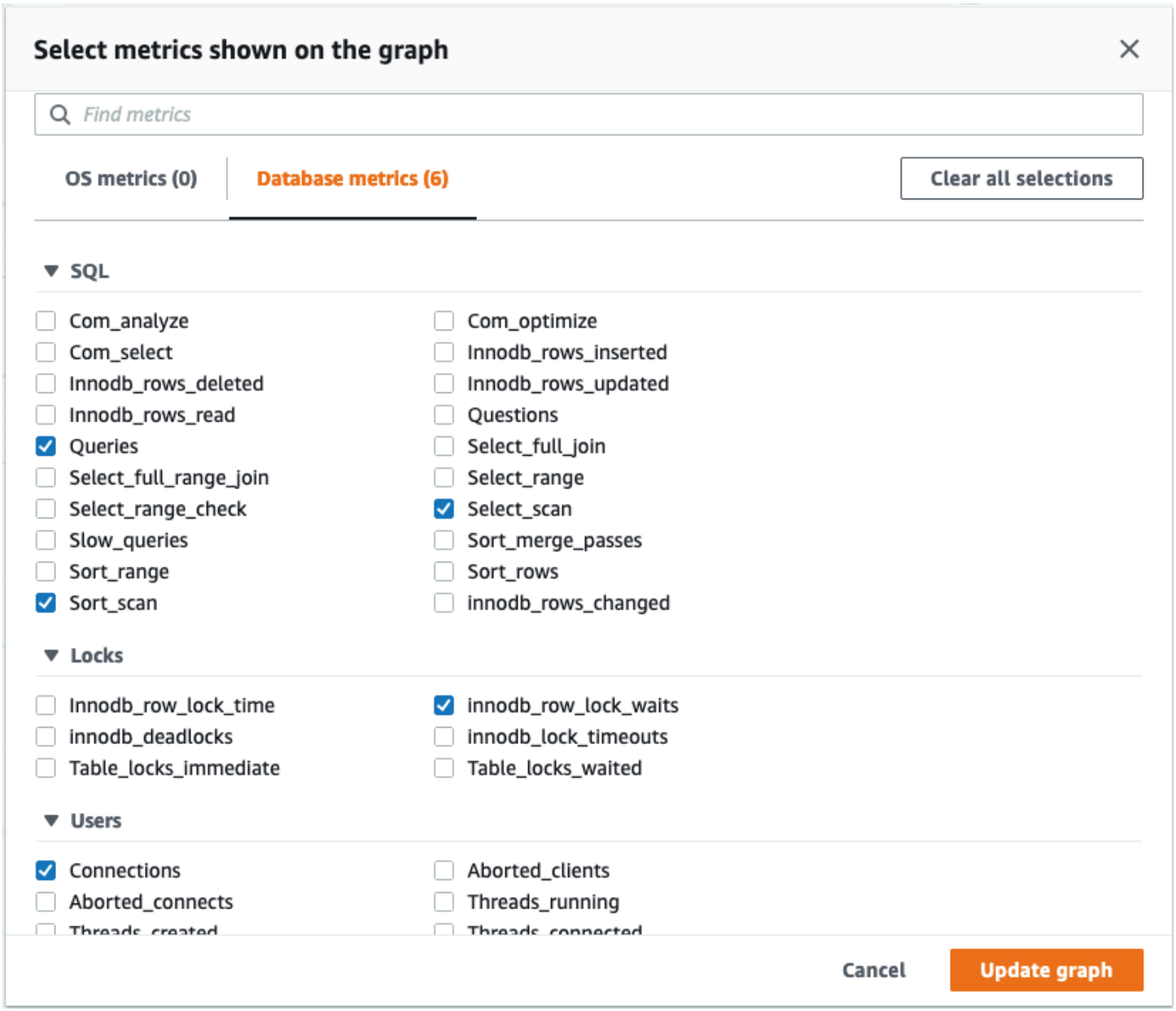
- Los contadores no nativos se definen mediante Amazon RDS. Puede obtener estas métricas mediante una consulta específica o derivarlas mediante dos o varias métricas nativas en los cálculos. Las métricas de contadores no nativos pueden representar latencias, ratios o tasas de aciertos. Por ejemplo:
  - `Cache.innoDB_buffer_pool_hits` representa el número de operaciones de lectura que podría recuperar InnoDB del conjunto de búferes sin utilizar el disco. Se calcula a partir de las métricas del contador nativo de la manera siguiente:

    ```
    db.Cache.Innodb_buffer_pool_read_requests - db.Cache.Innodb_buffer_pool_reads
    ```

  - `IO.innoDB_datafile_writes_to_disk` representa el número de operaciones de escritura del archivo de datos de InnoDB en el disco. Solo captura las operaciones en los archivos de datos, no las operaciones de escritura doble o registro redo de escritura. Se calcula como se indica a continuación:

    ```
    db.IO.Innodb_data_writes - db.IO.Innodb_log_writes - db.IO.Innodb_dblwr_writes
    ```

Puede visualizar las métricas de instancias de bases de datos directamente en el panel de Información de rendimiento. Elija Administrar métricas, elija la pestaña Métricas de la base de datos y, a continuación, seleccione las métricas que le interesen, como se muestra en la ilustración siguiente.



Elija el botón Actualizar gráfico para mostrar las métricas que seleccionó, tal y como se muestra en la ilustración siguiente.

Estadísticas de SQL

Información de rendimiento recopila métricas relacionadas con el rendimiento de las consultas SQL por cada segundo que se ejecuta una consulta y por cada llamada SQL. En general, Información de rendimiento recopila estadísticas de SQL por enunciado y resumen. Sin embargo, para las instancias de bases de datos de MariaDB y MySQL, las estadísticas solo se recopilan por resumen.

- Las estadísticas de resúmenes son una métrica compuesta de todas las consultas que tienen el mismo patrón pero que, en última instancia, tienen valores literales diferentes. El resumen reemplaza los valores literales específicos por una variable, por ejemplo:

```
SELECT department_id, department_name FROM departments WHERE location_id = ?
```

- Hay métricas que representan estadísticas por segundo para cada instrucción SQL resumida. Por ejemplo, `sql_tokenized.stats.count_star_per_sec` representa las llamadas por segundo (es decir, cuántas veces por segundo se ejecutó la instrucción SQL).

- Información de desempeño también incluye métricas que proporcionan estadísticas por llamada para una instrucción SQL. Por ejemplo, `sql_tokenized.stats.sum_timer_wait_per_call` muestra la latencia media de la instrucción SQL por llamada, en milisegundos.

Las estadísticas SQL están disponibles en el panel de Información de rendimiento, en la pestaña SQL principal de la tabla Dimensiones principales.

CloudWatch métricas para instancias de base de datos

Amazon CloudWatch también contiene métricas que Amazon RDS publica automáticamente. Las métricas que residen en el espacio de nombres `AWS/RDS` son métricas de instancias, que hacen referencia a la instancia (servicio) de Amazon RDS (es decir, al entorno de base de datos aislado que se ejecuta en la nube) y no a la instancia de base de datos en el sentido estricto del proceso mysqld. Por lo tanto, la mayoría de esas métricas predeterminadas pertenecen a la categoría de métricas del sistema operativo, según la definición estricta del término. Entre los ejemplos se incluyen `CPUUtilization`, `WriteIOPS`, `SwapUsage` y otros. Sin embargo, existen algunas métricas de instancias de bases de datos que son aplicables a MariaDB y MySQL:

- `BinLogDiskUsage`: cantidad de espacio en disco que ocupan los registros binarios.
- `DatabaseConnections`: número de conexiones de red de cliente a la instancia de base de datos.
- `ReplicaLag`: cantidad de retraso de una instancia de base de datos de réplica de lectura con respecto a la instancia de base de datos de origen.

Publicar métricas de Performance Insights en CloudWatch

Amazon RDS Performance Insights monitorea la mayoría de las métricas y dimensiones de las instancias de base de datos y las pone a disposición a través del panel Performance Insights de la consola AWS de administración. Este panel es ideal para la solución de problemas de bases de datos y el análisis de la causa de origen. Sin embargo, no es posible crear alarmas en Información de rendimiento para las métricas relacionadas con el rendimiento. Si desea crear alarmas basadas en las métricas de Performance Insights, esas métricas deben estar incluidas CloudWatch.

Performance Insights publica automáticamente las métricas en CloudWatch. Puede consultar los mismos datos de Performance Insights, pero tener las métricas integradas CloudWatch facilita la adición de CloudWatch alarmas y la adición de las métricas a los CloudWatch paneles existentes. Los contadores son métricas de rendimiento del sistema operativo y de la base de datos, como `os.memory.free` o `db.Locks.Innodb_row_lock_time`. La recopilación de métricas del sistema operativo depende de la configuración de Enhanced Monitoring. Si Enhanced Monitoring está desactivada, las métricas del sistema operativo se recopilan una vez por minuto. Si Enhanced Monitoring está activada, las métricas del sistema operativo se recopilan durante el periodo seleccionado. Para más información, consulte Activación y desactivación de Enhanced Monitoring en las preguntas frecuentes de Amazon RDS.

Performance Insights le permite exportar el panel de métricas preconfigurado o personalizado de su instancia de base de datos a CloudWatch. Puede exportar el panel de métricas como un panel nuevo o añadirlo a un CloudWatch panel existente. Al exportar el panel de métricas de Performance Insights al CloudWatch panel, obtendrá una visión unificada y holística del estado del sistema, ya que le proporcionará una visión general de las métricas asociadas a varios recursos del sistema, como las instancias EC2, los recursos de Amazon Elastic File System (Amazon EFS) y los recursos de Elastic Load Balancing (ELB), junto con las métricas de las instancias de base de datos.

Puede usar la función matemática CloudWatch `DB_PERF_INSIGHTS` métrica para consultar y crear alarmas y gráficos basados en las métricas de Performance Insights de CloudWatch. Para crear una alarma en una métrica de Performance Insights, siga las instrucciones de la CloudWatch documentación. Por ejemplo, si quiere activar una alarma cuando el total de transacciones activas en la instancia de bases de datos alcance un umbral específico, siga las instrucciones de esa página, utilice la siguiente expresión matemática `DB_PERF_INSIGHTS` y, a continuación, elija Aplicar:

```
DB_PERF_INSIGHTS('RDS', 'db-BQ2TPYY7HG2GDFC7APMB3BVB3M',
 'db.Transactions.active_transactions.avg')
```

donde `db-BQ2TPYY7HG2GDFC7APMB3BVB3M` es el id. del recurso de la instancia de bases de datos. Especifique el periodo (por ejemplo, 1 minuto) y las condiciones (por ejemplo, más de 1000). Para finalizar la creación de la alarma, configure las acciones de la alarma, agregue un nombre y una descripción, y obtenga una vista previa de la alarma y créela.

Supervisión del sistema operativo

Una instancia de base de datos en Amazon RDS para MySQL o MariaDB se ejecuta en el sistema operativo Linux, que utiliza los recursos del sistema subyacentes: CPU, memoria, red y almacenamiento.

```
MySQL [(none)]> SHOW variables LIKE 'version%';
+-------------------------+---------------------+
| Variable_name           | Value               |
+-------------------------+---------------------+
| version                 | 8.0.28              |
| version_comment         | Source distribution |
| version_compile_machine | aarch64             |
| version_compile_os      | Linux               |
| version_compile_zlib    | 1.2.11              |
+-------------------------+---------------------+
5 rows in set (0.00 sec)
```

El rendimiento general de la base de datos y del sistema operativo subyacente depende en gran medida del uso de los recursos del sistema. Por ejemplo, la CPU es el componente clave del rendimiento del sistema, ya que ejecuta las instrucciones del software de la base de datos y administra otros recursos del sistema. Si la CPU está sobreutilizada (es decir, si la carga requiere más potencia de la CPU que la aprovisionada para la instancia de base de datos), este problema afectaría al rendimiento y a la estabilidad de la base de datos y, en consecuencia, de la aplicación.

El motor de base de datos asigna y libera memoria de manera dinámica. Cuando no hay suficiente memoria en la RAM para hacer el trabajo actual, el sistema graba páginas de memoria en la memoria de intercambio, que se encuentra en el disco. Como el disco es mucho más lento que la memoria, incluso si el disco usa la tecnología SSD NVMe, la asignación excesiva de memoria provoca una degradación del rendimiento. El uso elevado de la memoria provoca un aumento de la latencia de las respuestas de la base de datos, ya que el tamaño de un archivo de paginación aumenta para admitir más memoria. Si la asignación de memoria es tan alta que agota los espacios de la RAM y la memoria de intercambio, es posible que el servicio de base de datos deje de estar disponible y los usuarios observen errores como `[ERROR] mysqld: Out of memory (Needed xyz bytes)`.

Los sistemas de administración de bases de datos de MySQL y MariaDB utilizan el subsistema de almacenamiento, que consta de discos que almacenan estructuras en el disco, como tablas,

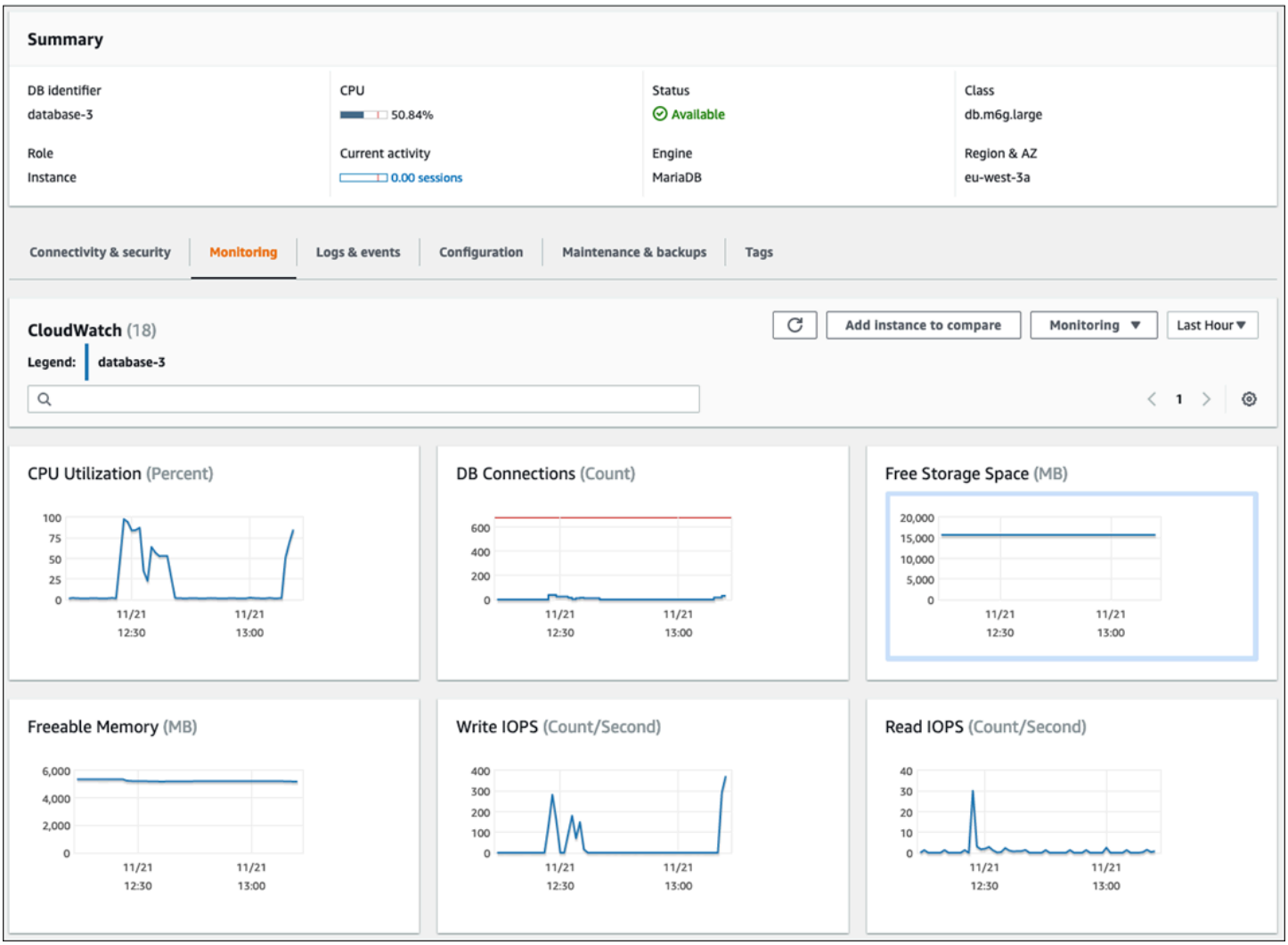
índices, registros binarios, registros de redo, registros de undo y archivos de búfer de doble escritura. Por lo tanto, la base de datos, a diferencia de otros tipos de software, debe llevar a cabo mucha actividad en el disco. Para obtener un funcionamiento óptimo de la base de datos, es importante que supervise y ajuste la utilización de E/S del disco y la asignación del espacio en disco. El rendimiento de la base de datos puede verse afectado cuando la base de datos alcanza las limitaciones del máximo de IOPS o del rendimiento que admite el disco. Por ejemplo, las ráfagas de acceso aleatorio ocasionadas por un análisis de índices pueden provocar una gran cantidad de operaciones de E/S por segundo, lo que, en última instancia, podría afectar a las limitaciones del almacenamiento subyacente. Es posible que los escaneos de tabla completa no alcancen el límite de IOPS, pero pueden provocar un alto rendimiento, que se mide en megabytes por segundo. Es fundamental supervisar y generar las alertas sobre la asignación de espacio en disco, ya que los errores como `OS error code 28: No space left on device` pueden provocar la falta de disponibilidad de la base de datos y dañarla.

Amazon RDS proporciona métricas en tiempo real para el sistema operativo en el que se ejecuta la instancia de base de datos. Amazon RDS publica de manera automática un conjunto de métricas del sistema operativo en CloudWatch. Estas métricas están disponibles para su visualización y análisis en la consola de Amazon RDS y en los paneles de CloudWatch. Puede configurar las alarmas en las métricas seleccionadas en CloudWatch. Entre los ejemplos se incluyen:

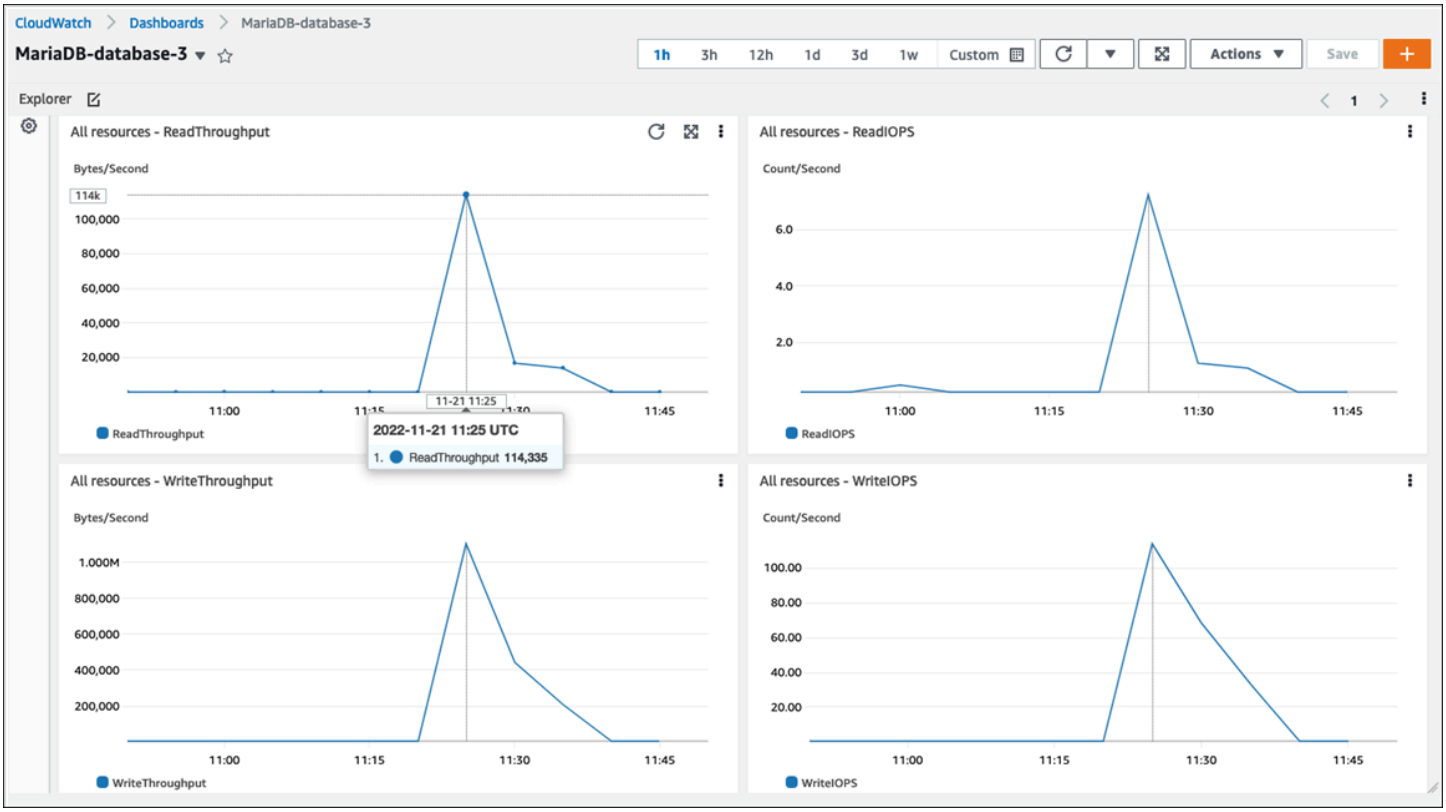
- `CPUUtilization`: porcentaje de uso de la CPU.
- `BinLogDiskUsage`: cantidad de espacio en disco que ocupan los registros binarios.
- `FreeableMemory`: cantidad de memoria de acceso aleatorio disponible. Representa el valor del campo `MemAvailable` de `/proc/meminfo`.
- `ReadIOPS`: número promedio de operaciones de E/S de lectura en disco por segundo.
- `WriteThroughput`: número promedio de bytes que se escribe en el disco por segundo del almacenamiento local.
- `NetworkTransmitThroughput`: tráfico de red de salida en el nodo de la base de datos, que combina el tráfico de la base de datos y el tráfico de Amazon RDS utilizado en la supervisión y la replicación.

Para obtener una referencia completa de todas las métricas publicadas por Amazon RDS en CloudWatch, consulte Métricas de Amazon CloudWatch para Amazon RDS en la documentación de Amazon RDS.

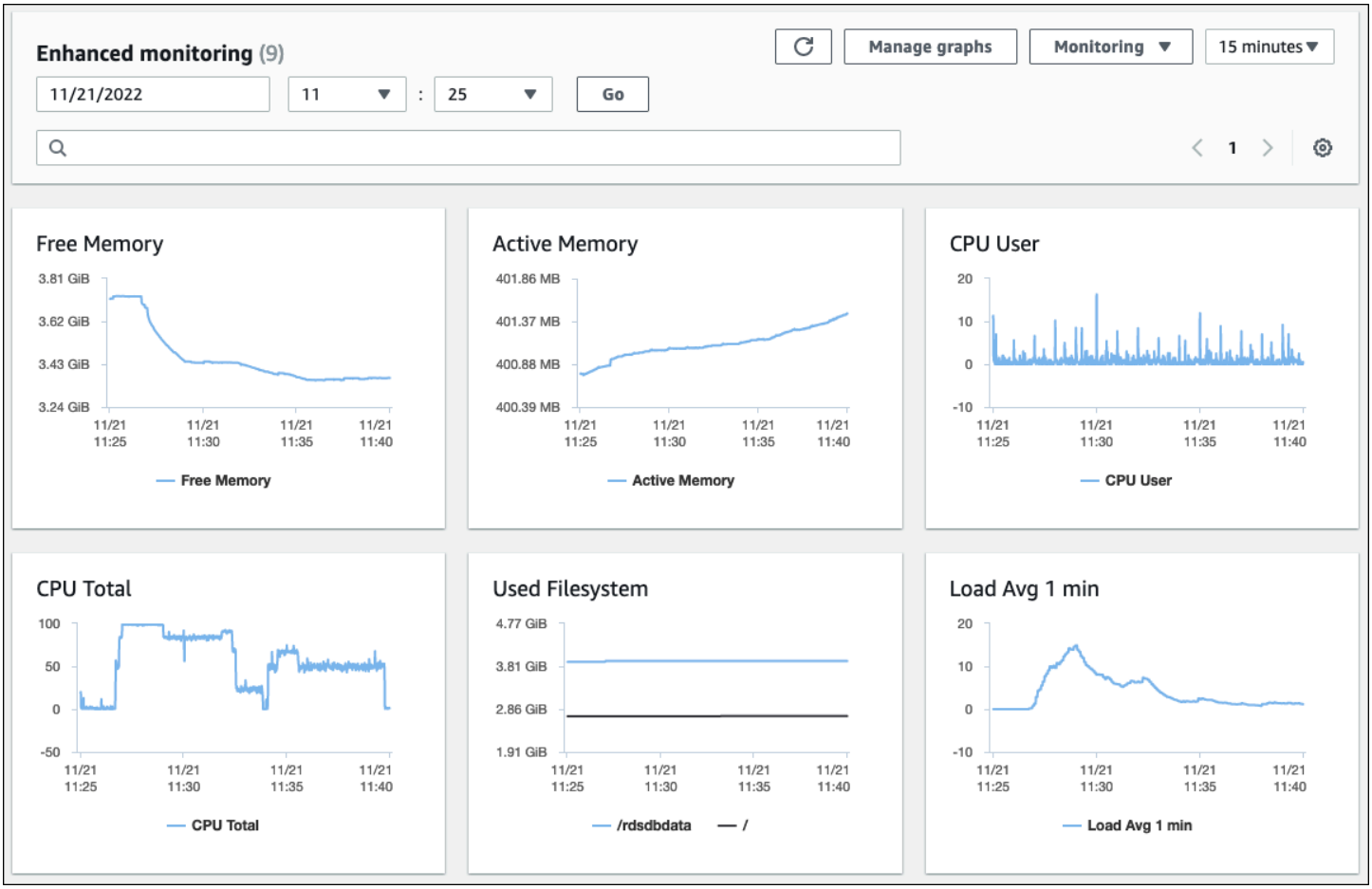
En el siguiente gráfico se muestran ejemplos de las métricas de CloudWatch para Amazon RDS que se muestran en la consola de Amazon RDS.



En el siguiente gráfico se muestran métricas similares que se muestran en el panel de CloudWatch.



Enhanced Monitoring para Amazon RDS recopila el otro conjunto de métricas del sistema operativo. Esta herramienta le ofrece una mayor visibilidad del estado de las instancias de base de datos de Amazon RDS para MariaDB y Amazon RDS para MySQL, ya que proporciona las métricas del sistema y la información sobre los procesos del sistema operativo en tiempo real. Cuando habilita Enhanced Monitoring en la instancia de base de datos y establece la granularidad deseada, la herramienta recopila las métricas del sistema operativo y la información del proceso, que puede mostrar y analizar en la consola de Amazon RDS, como se muestra en la siguiente pantalla.



Algunas de las métricas clave que proporciona Enhanced Monitoring son:

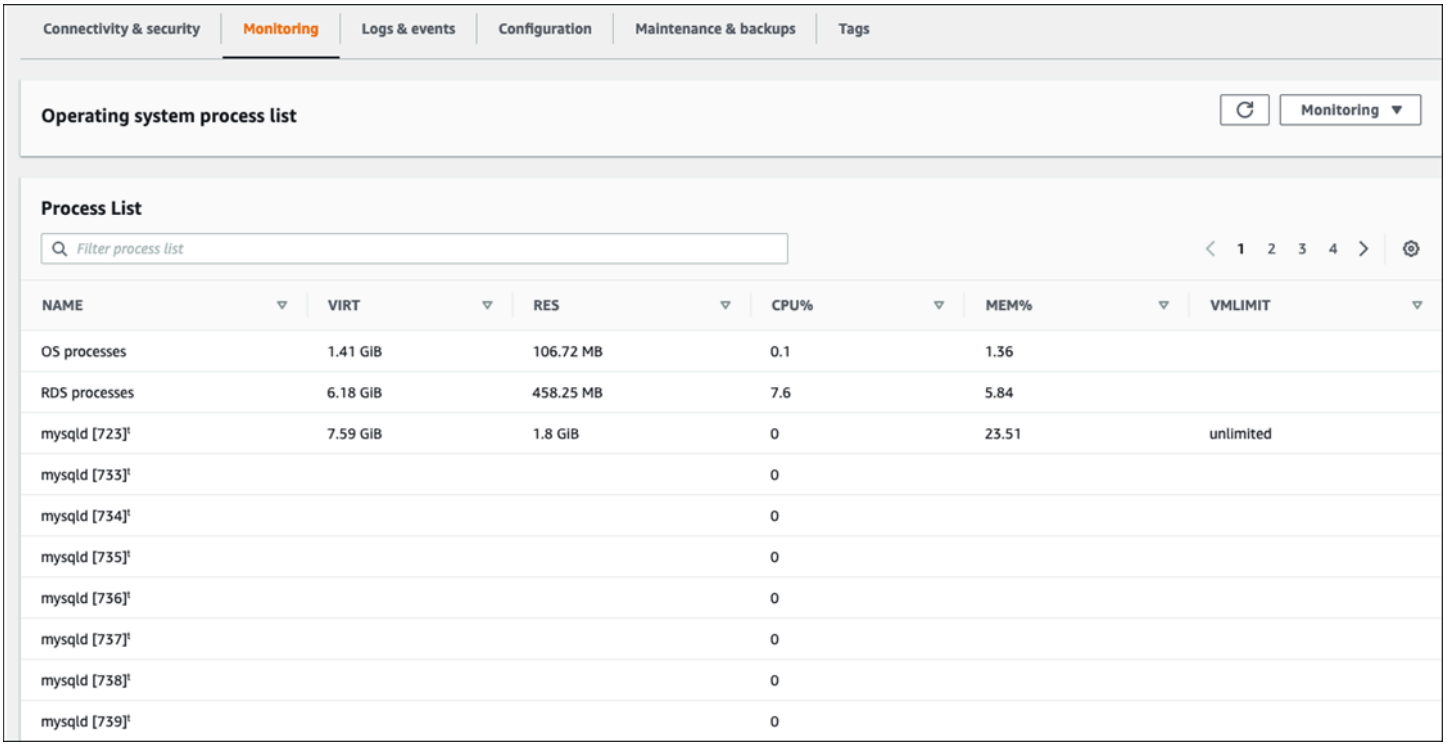
- `cpuUtilization.total`: porcentaje total de CPU utilizado.
- `cpuUtilization.user`: porcentaje de CPU utilizado por los programas de usuario.
- `memory.active`: cantidad de memoria asignada, en kilobytes.
- `memory.cached`: cantidad de memoria utilizada para almacenar en la caché las E/S basadas en el sistema de archivos.
- `loadAverageMinute.one`: número de procesos que solicitaron tiempo de la CPU durante el último minuto.

Para obtener una lista completa de las métricas, consulte Métricas del sistema operativo en Enhanced Monitoring en la documentación de Amazon RDS.

En la consola de Amazon RDS, la lista de procesos del sistema operativo proporciona detalles de cada proceso que se ejecuta en la instancia de base de datos. La lista está organizada en tres secciones:

- Procesos del sistema operativo: esta sección representa un resumen agregado de todos los procesos del núcleo y del sistema. Por lo general, estos procesos tienen un impacto mínimo en el rendimiento de la base de datos.
- Procesos de RDS: esta sección representa un resumen de los procesos de AWS necesarios para admitir una instancia de base de datos de Amazon RDS. Por ejemplo, incluye el agente de administración de Amazon RDS, los procesos de supervisión y diagnóstico y procesos similares.
- Procesos secundarios de RDS: esta sección representa un resumen de los procesos de Amazon RDS que admiten la instancia de base de datos, en este caso, el proceso `mysqld` y sus subprocesos. Los subprocesos de `mysqld` aparecen anidados debajo del proceso principal `mysqld`.

En la ilustración siguiente de la pantalla se muestra la lista de procesos del sistema operativo en la consola de Amazon RDS.

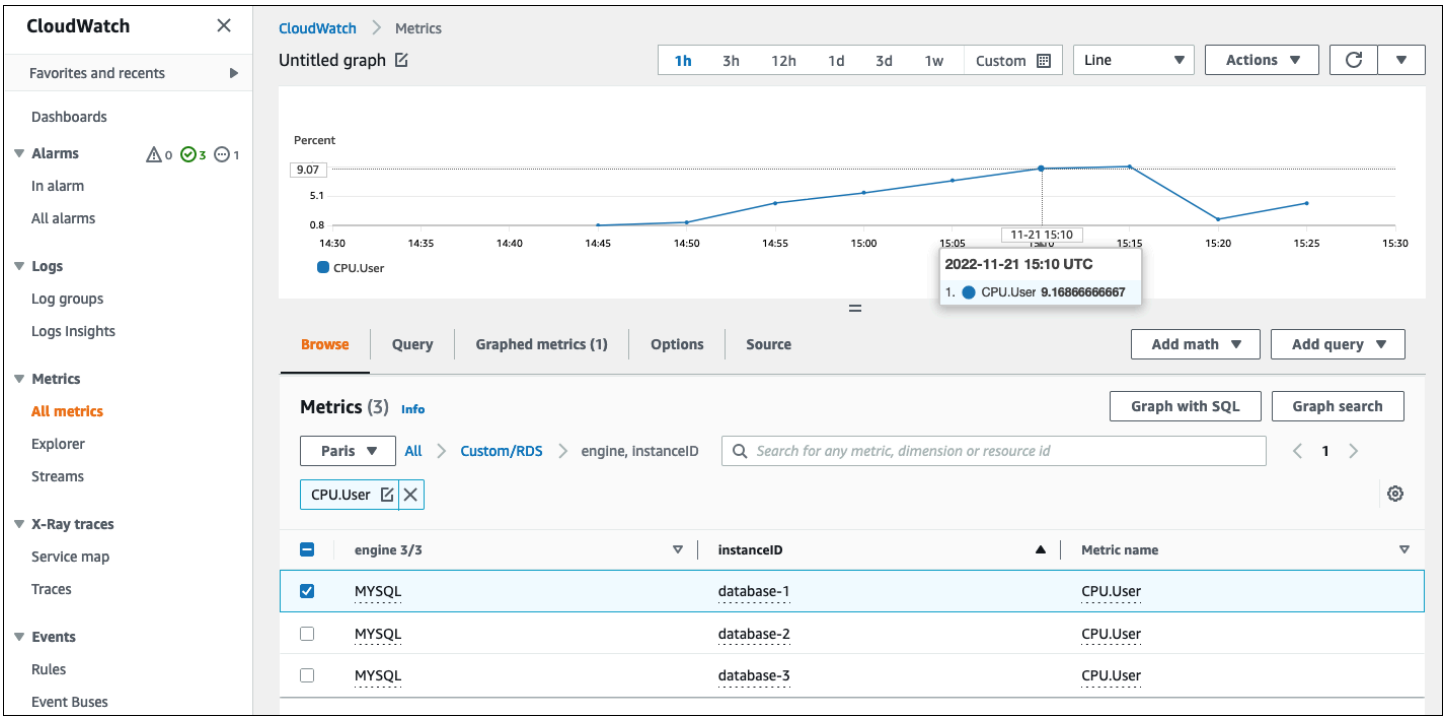


Amazon RDS envía las métricas de Enhanced Monitoring a su cuenta de Registros de CloudWatch. Los datos de supervisión que se muestran en la consola de Amazon RDS se obtienen de Registros

de CloudWatch. También puede obtener las métricas de una instancia de base de datos en forma de flujo de registro de Registros de CloudWatch. Estas métricas se almacenan en formato JSON. Además, puede consumir la salida JSON de monitorización mejorada desde registros de Amazon Cloudwatch en un sistema de monitoreo de su elección.

Para mostrar los gráficos en el panel de CloudWatch y crear las alarmas que inicien una acción si una métrica supera el umbral definido, debe crear los filtros de las métricas en CloudWatch a partir de Registros de CloudWatch. Para obtener instrucciones detalladas, consulte el artículo de AWS re:Post sobre cómo filtrar los registros de Registros de CloudWatch de Enhanced Monitoring para generar las métricas personalizadas automatizadas para Amazon RDS.

El siguiente ejemplo ilustra la métrica personalizada `CPU.User` en el espacio de nombres `Custom/RDS`. Esta métrica personalizada se crea al filtrar la métrica de Enhanced Monitoring `cpuUtilization.user` de Registros de CloudWatch.



Cuando la métrica está disponible en el repositorio de CloudWatch, puede mostrarla y analizarla en los paneles de CloudWatch, aplicar más operaciones matemáticas y de consulta y configurar una alarma para supervisar esta métrica concreta y generar alertas si los valores observados no se ajustan a las condiciones de alarma definidas.

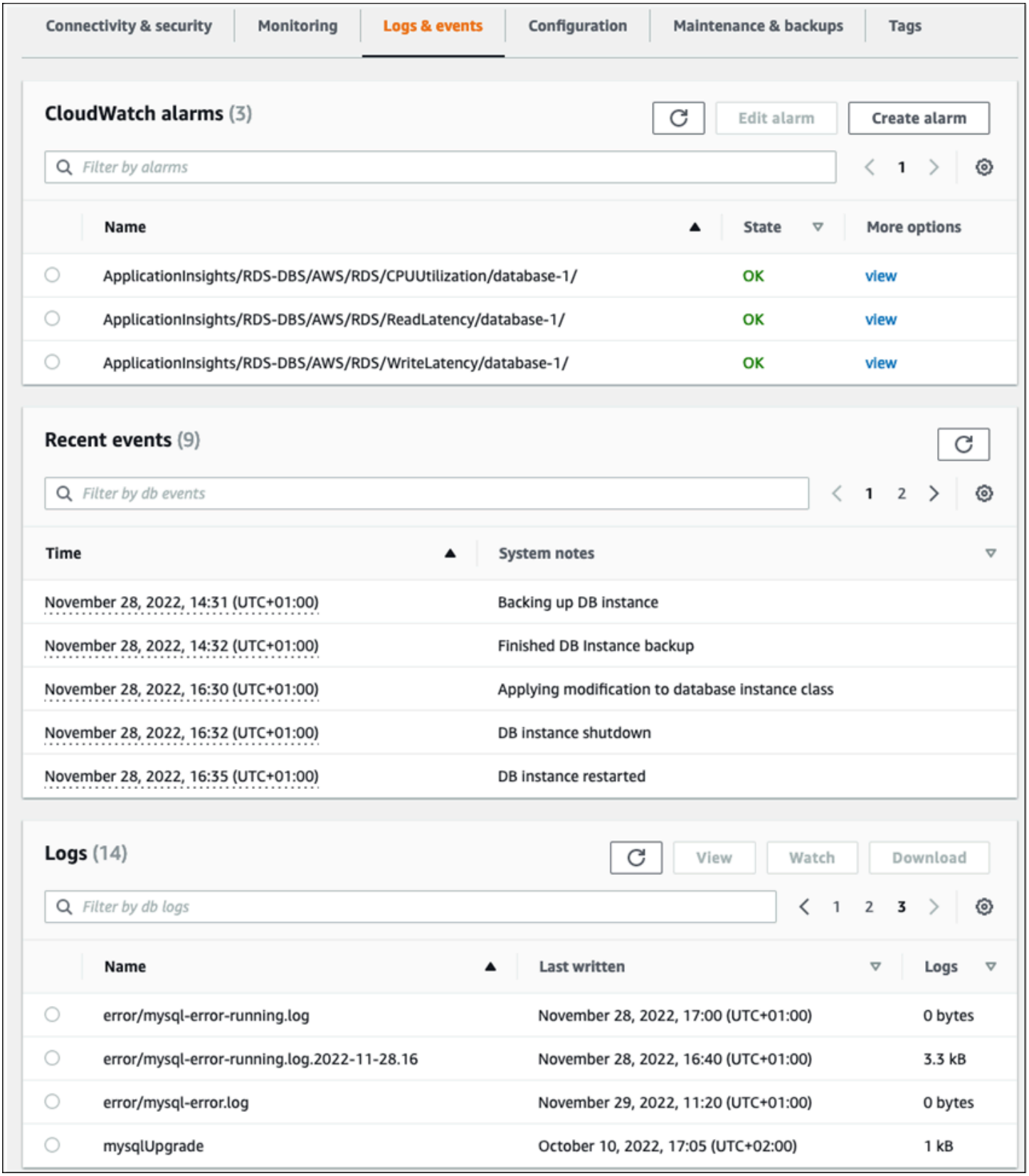
Eventos, registros y registros de auditoría

Supervisar las métricas de las instancias de base de datos y las métricas del sistema operativo, analizar las tendencias y comparar las métricas con los valores de la línea de base y generar alertas cuando los valores superen los umbrales definidos son prácticas recomendadas necesarias para lograr y mantener la fiabilidad, la disponibilidad, el rendimiento y la seguridad de las instancias de bases de datos de Amazon RDS. Sin embargo, una solución completa también debe supervisar los eventos, los archivos de registro y los registros de auditoría de las bases de datos de MySQL y MariaDB.

Secciones

Eventos de Amazon RDS

Un evento de Amazon RDS indica un cambio en el entorno de Amazon RDS. Por ejemplo, cuando el estado de la instancia de bases de datos cambia de Empezando a Disponible, Amazon RDS genera el evento `RDS-EVENT-0088 The DB instance has been started`. Amazon RDS envía eventos a Amazon EventBridge casi en tiempo real. Puede acceder a los eventos a través de la consola de Amazon RDS, el comando de la AWS CLI describe-events o la operación DescribeEvents de la API de Amazon RDS. La siguiente ilustración de pantalla muestra los eventos y registros que se muestran en la consola de Amazon RDS.


Connectivity & security
Monitoring
Logs & events
Configuration
Maintenance & backups
Tags
CloudWatch alarms (3)
Edit alarm
Create alarm
Filter by alarms
1
Name
State
More options
ApplicationInsights/RDS-DBS/AWS/RDS/CPUUtilization/database-1/
OK
view
ApplicationInsights/RDS-DBS/AWS/RDS/ReadLatency/database-1/
OK
view
ApplicationInsights/RDS-DBS/AWS/RDS/WriteLatency/database-1/
OK
view
Recent events (9)
Filter by db events
1
2
Time
System notes
November 28, 2022, 14:31 (UTC+01:00)
Backing up DB instance
November 28, 2022, 14:32 (UTC+01:00)
Finished DB Instance backup
November 28, 2022, 16:30 (UTC+01:00)
Applying modification to database instance class
November 28, 2022, 16:32 (UTC+01:00)
DB instance shutdown
November 28, 2022, 16:35 (UTC+01:00)
DB instance restarted
Logs (14)
View
Watch
Download
Filter by db logs
1
2
3
Name
Last written
Logs
error/mysql-error-running.log
November 28, 2022, 17:00 (UTC+01:00)
0 bytes
error/mysql-error-running.log.2022-11-28.16
November 28, 2022, 16:40 (UTC+01:00)
3.3 kB
error/mysql-error.log
November 29, 2022, 11:20 (UTC+01:00)
0 bytes
mysqlUpgrade
October 10, 2022, 17:05 (UTC+02:00)
1 kB

Amazon RDS emite distintos tipos de eventos, entre ellos los eventos de instancias de bases de datos, los eventos de grupos de parámetros de bases de datos, los eventos de grupos de seguridad de base de datos, los eventos de instantáneas de bases de datos, los eventos de proxy de RDS y los eventos de implementación azul/verde. La información incluye lo siguiente:

- Nombre y tipo de origen, por ejemplo: `"SourceIdentifier": "database-1", "SourceType": "db-instance"`
- Fecha y hora del evento, por ejemplo: `"Date": "2022-12-01T09:20:28.595000+00:00"`
- Mensaje asociado al evento, por ejemplo: `"Message": "Finished updating DB parameter group"`
- Categoría de evento, por ejemplo: `"EventCategories": ["configuration change"]`

Para obtener una referencia completa, consulte Categorías de eventos de Amazon RDS y mensajes de eventos en la documentación de Amazon RDS.

Le recomendamos que supervise los eventos de Amazon RDS, ya que estos indican cambios de estado en la disponibilidad de las instancias de base de datos, cambios de configuración, cambios de estado de réplica de lectura, eventos de copias de seguridad y recuperación, acciones de conmutación por error, eventos de error, modificaciones en los grupos de seguridad y muchas otras notificaciones. Por ejemplo, si configuró una instancia de bases de datos de réplica de lectura para mejorar el rendimiento y la durabilidad de la base de datos, le recomendamos que supervise los eventos de Amazon RDS para la categoría de eventos de réplica de lectura asociada a las instancias de base de datos. Esto se debe a eventos, tales como `RDS-EVENT-0057 Replication on the read replica was terminated`, indican que la réplica de lectura ya no se sincroniza con la instancia de base de datos principal. Una notificación al equipo responsable de que se produjo un evento de este tipo podría ayudar a mitigar el problema a tiempo. Amazon EventBridge y otros Servicios de AWS, como AWS Lambda, Amazon Simple Queue Service (Amazon SQS) y Amazon Simple Notification Service (Amazon SNS), pueden ayudar a automatizar las respuestas a eventos del sistema, como problemas de disponibilidad de la base de datos o cambios de recursos.

En la consola de Amazon RDS, puede recuperar eventos de las últimas 24 horas. Si utiliza la AWS CLI o la API de Amazon RDS para ver eventos, puede recuperar los de últimos 14 días. Para ello, utilice el comando describe-events de la manera siguiente.

```
$ aws rds describe-events --source-identifier database-1 --source-type db-instance
{
    "Events": [
```

```
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "CloudWatch Logs Export enabled for logs [audit, error, general,
 slowquery]",
            "EventCategories": [],
            "Date": "2022-12-01T09:20:28.595000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        },
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "Finished updating DB parameter group",
            "EventCategories": [
                "configuration change"
            ],
            "Date": "2022-12-01T09:22:40.413000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        }
    ]
}
```

Si desea almacenar eventos a largo plazo, ya sea hasta el periodo de vencimiento especificado o de forma permanente, puede utilizar Registros de CloudWatch para registrar la información sobre los eventos generados por Amazon RDS. Para implementar esta solución, puede utilizar un tema de Amazon SNS para recibir notificaciones de los eventos de Amazon RDS y, a continuación, llamar a una función de Lambda para registrar el evento en Registros de CloudWatch.

1. Cree una función de Lambda a la que se invoque en el evento y registre la información del evento en Registros de CloudWatch. Registros de CloudWatch está integrado con Lambda y proporciona una forma práctica de registrar la información de los eventos de registro, mediante la función de impresión para `stdout`.
2. Cree un tema de SNS con una suscripción a una función de Lambda (establezca Protocolo en Lambda) y establezca Punto de conexión en el nombre de recurso de Amazon (ARN) de la función de Lambda que creó en el paso anterior.
3. Configure el tema de SNS para recibir las notificaciones de los eventos de Amazon RDS. Para obtener instrucciones detalladas, consulte el artículo de AWS re:Post sobre cómo hacer que el tema de Amazon SNS reciba las notificaciones de Amazon RDS.

4. En la consola de Amazon RDS, cree una nueva suscripción a eventos. Establezca Destino en el ARN y, a continuación, seleccione el tema de SNS que creó anteriormente. Establezca Tipo de origen y Categorías de eventos que incluir según sus requisitos. Para más información, consulte Suscripción a la notificación de eventos de Amazon RDS en la documentación de Amazon RDS.

Registros de la base de datos

Las bases de datos de MySQL y MariaDB generan registros a los que puede acceder para hacer auditorías y solucionar problemas. Estos registros son:

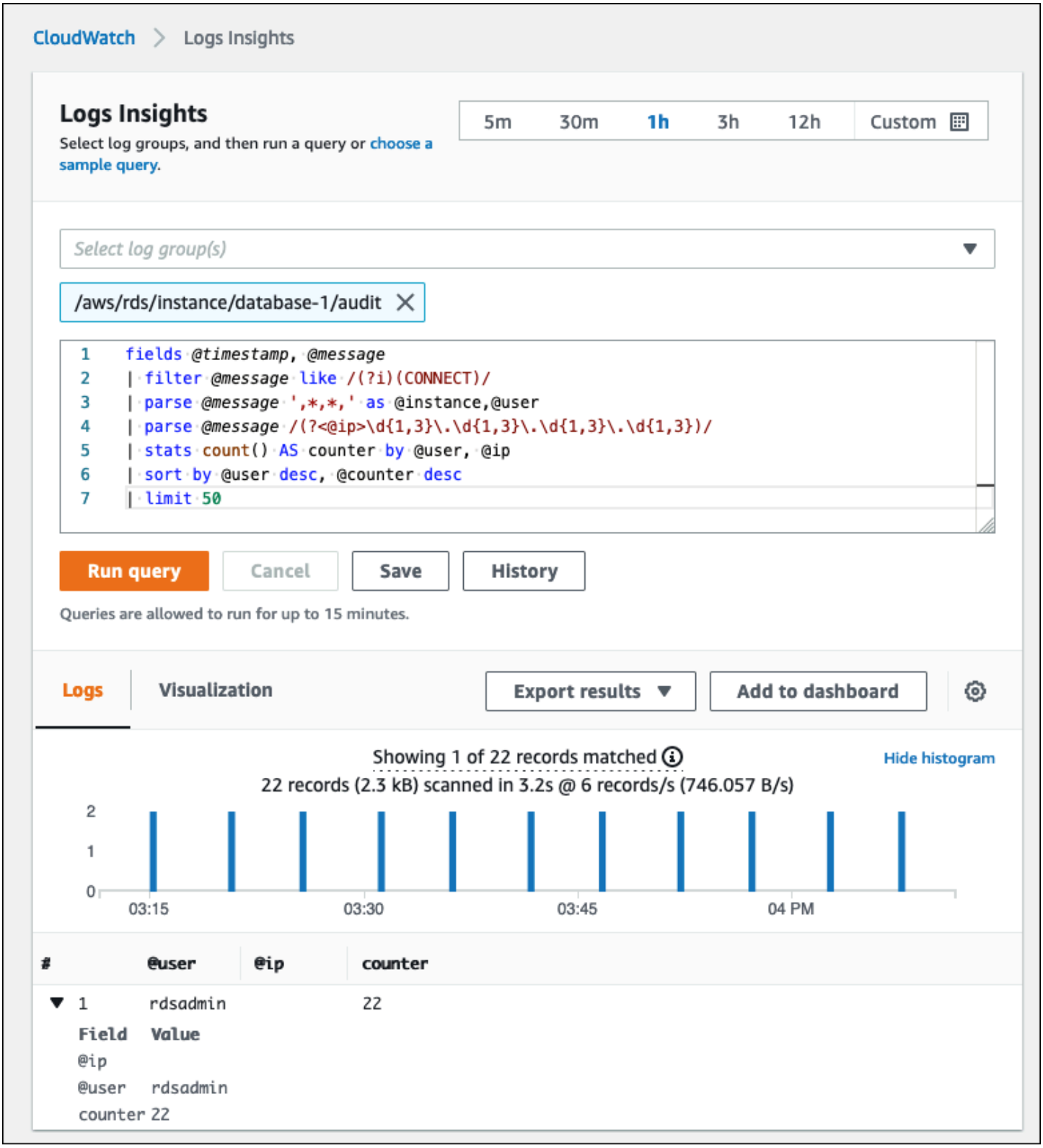
- Auditoría: el registro de auditoría es un conjunto de registros que registran la actividad del servidor. Para cada sesión de cliente, registra quién se conectó al servidor (nombre de usuario y host), qué consultas se ejecutaron, a qué tablas se accedió y qué variables del servidor se cambiaron.
- Error: este registro contiene las horas de inicio y apagado del servidor (`mysqld`) y los mensajes de diagnóstico, como errores, advertencias y notas, producidos durante el inicio y el apagado del servidor y mientras el servidor está en ejecución.
- General: este registro registra la actividad de `mysqld`, tal como la actividad de conexión y desconexión de cada cliente, así como las consultas SQL recibidas de los clientes. El registro de consultas general puede resultar muy útil cuando se sospecha que se produjo un error y se quiere saber exactamente qué envió el cliente a `mysqld`.
- Consulta lenta: este registro proporciona un registro de las consultas SQL que tardaron mucho tiempo en llevarse a cabo.

Como práctica recomendada, debe publicar los registros de bases de datos de Amazon RDS en Registros de Amazon CloudWatch. Con Registros de CloudWatch puede hacer análisis de los datos del registro en tiempo real, guardarlos en un almacenamiento de larga duración y administrarlos con el agente de Registros de CloudWatch. Puede acceder a los registros de la base de datos y verlos desde la consola de Amazon RDS. También puede utilizar Información de registros de CloudWatch para buscar y analizar de forma interactiva los datos de registros en Registros de CloudWatch. El siguiente ejemplo ilustra una consulta en el registro de auditoría que verifica cuántas veces aparecen los eventos `CONNECT` en el registro, quién se conectó y desde qué cliente (dirección IP) se conectó. El extracto del registro de auditoría podría tener el aspecto siguiente:

```
20221201 14:07:05,ip-10-22-1-51,rdsadmin,localhost,821,0,CONNECT,,,0,SOCKET
20221201 14:07:05,ip-10-22-1-51,rdsadmin,localhost,821,0,DISCONNECT,,,0,SOCKET
20221201 14:12:20,ip-10-22-1-51,rdsadmin,localhost,822,0,CONNECT,,,0,SOCKET
```

```
20221201 14:12:20,ip-10-22-1-51,rdsadmin,localhost,822,0,DISCONNECT,,,0,SOCKET
20221201 14:17:35,ip-10-22-1-51,rdsadmin,localhost,823,0,CONNECT,,,0,SOCKET
20221201 14:17:35,ip-10-22-1-51,rdsadmin,localhost,823,0,DISCONNECT,,,0,SOCKET
20221201 14:22:50,ip-10-22-1-51,rdsadmin,localhost,824,0,CONNECT,,,0,SOCKET
20221201 14:22:50,ip-10-22-1-51,rdsadmin,localhost,824,0,DISCONNECT,,,0,SOCKET
```

La consulta de ejemplo de Información de registros muestra que `rdsadmin` se conectó a la base de datos de `localhost` cada 5 minutos, un total de 22 veces, como se muestra en la ilustración siguiente. Estos resultados indican que la actividad se originó a partir de los procesos internos de Amazon RDS, como el propio sistema de supervisión.



Los eventos de registro suelen incluir mensajes importantes que es conveniente tener en cuenta, como advertencias o errores sobre las operaciones asociadas a las instancias de bases de datos

de MySQL y MariaDB. Por ejemplo, si una operación falla, puede producirse un error y registrarse en el archivo de registro de errores de la siguiente manera: `ERROR 1114 (HY000): The table zip_codes is full`. Es posible que quiera supervisar estas entradas para comprender la evolución de los errores. Puede crear métricas personalizadas de CloudWatch a partir de los registros de Amazon RDS mediante filtros que permiten supervisar de manera automática los registros de la base de datos de Amazon RDS, supervisar un registro específico para detectar patrones específicos y generar una alarma si se producen infracciones del comportamiento esperado. Por ejemplo, cree un filtro de métricas para el grupo de registros `/aws/rds/instance/database-1/error` que supervise el registro de errores y busque el patrón específico, como `ERROR`. Establezca Patrón de filtro en `ERROR` y Valor de métricas en`1`. El filtro detectará todos los registros que contengan la palabra clave `ERROR` y aumentará el recuento en 1 por cada evento de registro que contenga la palabra “ERROR”. Después de crear el filtro, puede establecer una alarma para que le notifique en caso de que se detecten errores en el registro de errores de MySQL o MariaDB.

Para más información sobre la supervisión del registro de consultas y los registros de errores lentos mediante la creación de un panel de CloudWatch y mediante Información de registros de CloudWatch, consulte la publicación de blog Creación de un panel de Amazon CloudWatch para supervisar Amazon RDS y Amazon Aurora MySQL.

Registros de seguimiento de auditoría

El registro de auditoría proporciona un registro cronológico y relevante para la seguridad de los eventos que se producen en su Cuenta de AWS. Incluye eventos para Amazon RDS que proporcionan pruebas documentales de la secuencia de actividades que afectaron a la base de datos o al entorno de nube. En Amazon RDS para MySQL o MariaDB, el uso del registro de auditoría implica:

- Supervisión del registro de auditoría de la instancia de bases de datos
- Supervisión de las llamadas a la API de Amazon RDS en AWS CloudTrail

En el caso de una instancia de bases de datos de Amazon RDS, los objetivos de la auditoría suelen incluir lo siguiente:

- Habilitar la responsabilidad de lo siguiente:
  - Modificaciones hechas en el parámetro o la configuración de seguridad

  - Acciones hechas en un esquema, tabla o fila de una base de datos, o acciones que afectan a un contenido específico
- Detección e investigación de intrusiones
- Detección e investigación de actividades sospechosas
- Detección de problemas de autorización, por ejemplo, para identificar abusos en los derechos de acceso por parte de usuarios habituales o con privilegios

El registro de auditoría de la base de datos intenta responder a estas preguntas típicas: ¿Quién vio o modificó la información confidencial de la base de datos? ¿Cuándo sucedió esto? ¿Desde dónde accedió un usuario específico a los datos? ¿Los usuarios privilegiados abusaron de sus derechos de acceso ilimitado?

MySQL y MariaDB implementan la característica de registro de auditoría de la instancia de bases de datos mediante el complemento de auditoría de MariaDB. Este complemento registra la actividad de la base de datos, como el registro de los usuarios en la base de datos y las consultas que se ejecutan en la base de datos. El registro de la actividad de la base de datos se almacena en un archivo de registro. Para acceder al registro de auditoría, la instancia de base de datos debe usar un grupo de opciones personalizado con la opción `MARIADB_AUDIT_PLUGIN`. Para más información, consulte Compatibilidad del complemento de auditoría de MariaDB para MySQL en la documentación de Amazon RDS. Las entradas del registro de auditoría se almacenan en un formato específico, según lo define el complemento. Puede encontrar más detalles acerca del formato del registro de auditoría en la documentación del servidor de MariaDB.

El registro de auditoría de Nube de AWS para su cuenta de AWS se proporciona mediante el servicio AWS CloudTrail. CloudTrail captura las llamadas a la API de Amazon RDS como eventos. Todas las acciones de Amazon RDS se registran. CloudTrail proporciona un registro de las acciones en Amazon RDS que hace un usuario, un rol u otro servicio de AWS. Los eventos incluyen las acciones llevadas a cabo en la Consola de administración de AWS, la AWS CLI y los SDK y API de AWS

Ejemplo

En un escenario de una auditoría típica, es posible que tenga que combinar los registros de AWS CloudTrail con el registro de auditoría de la base de datos y la supervisión de eventos de Amazon RDS. Por ejemplo, podría tener un escenario en el que los parámetros de la base de datos de la instancia de bases de datos de Amazon RDS (por ejemplo `database-1`) se hayan modificado

y la tarea consista en identificar quién hizo la modificación, qué se cambió y cuándo se produjo el cambio.

Para llevar a cabo la tarea, haga esto:

1. Enumere los eventos de Amazon RDS que se produjeron en la instancia de base de datos `database-1` y determine si hay algún evento en la categoría `configuration change` que contiene el mensaje `Finished updating DB parameter group`.

```
$ aws rds describe-events --source-identifier database-1 --source-type db-instance
{
    "Events": [
        {
            "SourceIdentifier": "database-1",
            "SourceType": "db-instance",
            "Message": "Finished updating DB parameter group",
            "EventCategories": [
                "configuration change"
            ],
            "Date": "2022-12-01T09:22:40.413000+00:00",
            "SourceArn": "arn:aws:rds:eu-west-3:111122223333:db:database-1"
        }
    ]
}
```

2. Identifique el grupo de parámetros de base de datos que utiliza la instancia de base de datos:

```
$ aws rds describe-db-instances --db-instance-identifier database-1 --query
 'DBInstances[*].[DBInstanceIdentifier,Engine,DBParameterGroups]'
[
    [
        "database-1",
        "mariadb",
        [
            {
                "DBParameterGroupName": "mariadb10-6-test",
                "ParameterApplyStatus": "pending-reboot"
            }
        ]
    ]
]
```

3. Utilice la AWS CLI para buscar los eventos de CloudTrail en la región en la que se implementó `database-1`, en el periodo cercano al evento de Amazon RDS detectado en el paso 1 y donde `EventName=ModifyDBParameterGroup`.

```
$ aws cloudtrail --region eu-west-3 lookup-events --lookup-attributes
 AttributeKey=EventName,AttributeValue=ModifyDBParameterGroup --start-time
 "2022-12-01, 09:00 AM" --end-time "2022-12-01, 09:30 AM"

{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Role1",
                "accountId": "111122223333",
                "userName": "User1"
            }
        }
    },
    "eventTime": "2022-12-01T09:18:19Z",
    "eventSource": "rds.amazonaws.com",
    "eventName": "ModifyDBParameterGroup",
    "awsRegion": "eu-west-3",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "parameters": [
            {
                "isModifiable": false,
                "applyMethod": "pending-reboot",
                "parameterName": "innodb_log_buffer_size",
                "parameterValue": "8388612"
            },
            {
                "isModifiable": false,
                "applyMethod": "pending-reboot",
                "parameterName": "innodb_write_io_threads",
                "parameterValue": "8"
            }
```

```
        ],
        "dBParameterGroupName": "mariadb10-6-test"
    },
    "responseElements": {
        "dBParameterGroupName": "mariadb10-6-test"
    },
    "requestID": "fdf19353-de72-4d3d-bf29-751f375b6378",
    "eventID": "0bba7484-0e46-4e71-93a8-bd01ca8386fe",
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "sessionCredentialFromConsole": "true"
}
```


El evento de CloudTrail revela que `User1` con el rol `Role1` de la cuenta de AWS 111122223333 modificó el grupo de parámetros de base de datos `mariadb10-6-test`, que utilizaba la instancia de bases de datos `database-1` en `2022-12-01 at 09:18:19 h`. Se modificaron dos parámetros y se establecieron en los siguientes valores:

- `innodb_log_buffer_size = 8388612`
- `innodb_write_io_threads = 8`

Características adicionales de CloudTrail y Registros de CloudWatch

Puede resolver los problemas operativos y los incidentes de seguridad durante los últimos 90 días con Historial de eventos en la consola de CloudTrail. Para ampliar el periodo de retención y aprovechar las funcionalidades de consulta adicionales, puede utilizar AWS CloudTrail Lake. Con AWS CloudTrail Lake, puede conservar los datos de los eventos en un almacén de datos de eventos durante hasta siete años. Además, el servicio admite consultas SQL complejas que ofrecen una vista más detallada y personalizable de los eventos que las vistas proporcionadas por las búsquedas de clave-valor sencillas en Historial de eventos.

Para supervisar los registros de auditoría, configurar las alarmas y recibir las notificaciones cuando se produzca una actividad específica, debe configurar CloudTrail para que envíe sus registros de seguimiento a Registros de CloudWatch. Después de almacenar los registros de seguimiento como Registros de CloudWatch, puede definir los filtros de las métricas para evaluar los eventos de registro para que coincidan con los términos, las frases o los valores, y asignar métricas a los

filtros de las métricas. Además, puede crear alarmas de CloudWatch que se generan de acuerdo con los umbrales y los periodos especificados. Por ejemplo, puede configurar alarmas que envíen notificaciones a los equipos responsables, para que puedan tomar las medidas adecuadas. También puede configurar CloudWatch para que realice de forma automática una acción en respuesta a una alarma.

Alertas

Las alertas son unos de los orígenes de información más importantes en materia de seguridad, disponibilidad, rendimiento y fiabilidad de la infraestructura y los servicios de TI. Notifican e informan a los equipos de TI sobre las amenazas de seguridad actuales, las interrupciones, los problemas de rendimiento o los errores del sistema.

La Biblioteca de Infraestructura de Tecnología de la Información (ITIL), en concreto las prácticas de administración de servicios de TI (ITSM), establece las alertas automatizadas como el punto central de las prácticas recomendadas de supervisión y administración de eventos y administración de incidentes.

Las alertas de incidentes se producen cuando las herramientas de supervisión generan alertas para notificar al equipo y a las herramientas automatizadas (en el caso de los elementos que se pueden procesar automáticamente) sobre cambios, acciones de alto riesgo o errores en el entorno de TI. Las alertas de TI son la primera línea de defensa contra las interrupciones del sistema o los cambios que pueden convertirse en incidentes graves. Al supervisar automáticamente los sistemas y generar alertas en caso de interrupciones y cambios riesgosos, los equipos de TI pueden minimizar el tiempo de inactividad y reducir los altos costos que conlleva.

Como prácticas recomendadas, el AWS Well-Architected Framework prescribe que utilice la supervisión para generar notificaciones basadas en alarmas y que supervise y alarme de forma proactiva. Utilice CloudWatch un servicio de monitoreo externo para configurar alarmas que indiquen cuándo las métricas están fuera de los límites esperados.

El objetivo de la administración de alertas es establecer procedimientos estandarizados y eficientes para administrar los eventos e incidentes relacionados con TI mediante el registro, la clasificación, la definición e implementación de las acciones, el cierre y las actividades de revisión posteriores a los incidentes.

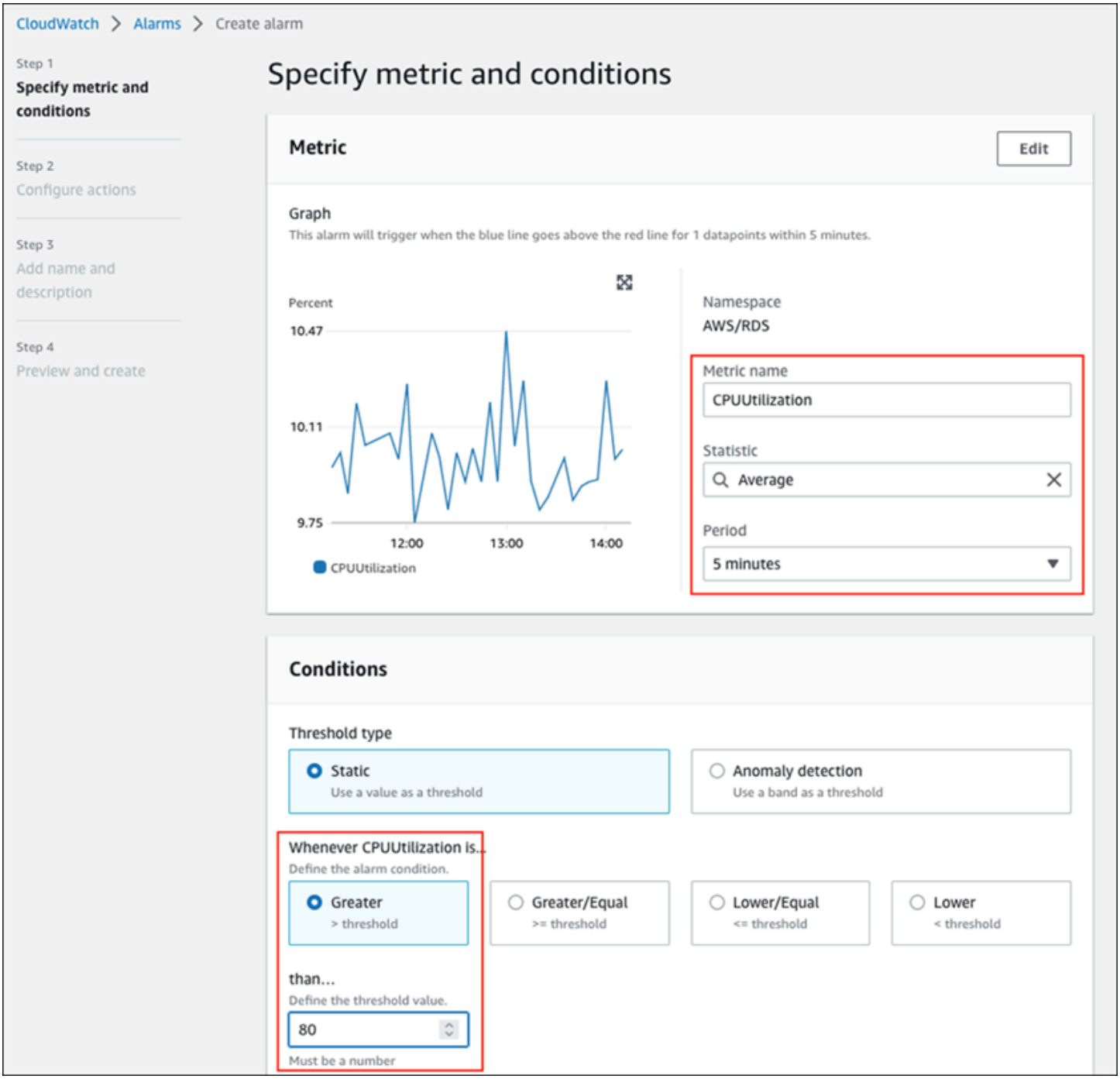
Secciones

- CloudWatch alarmas
- EventBridge reglas
- Especificar las acciones y activar y desactivar las alarmas

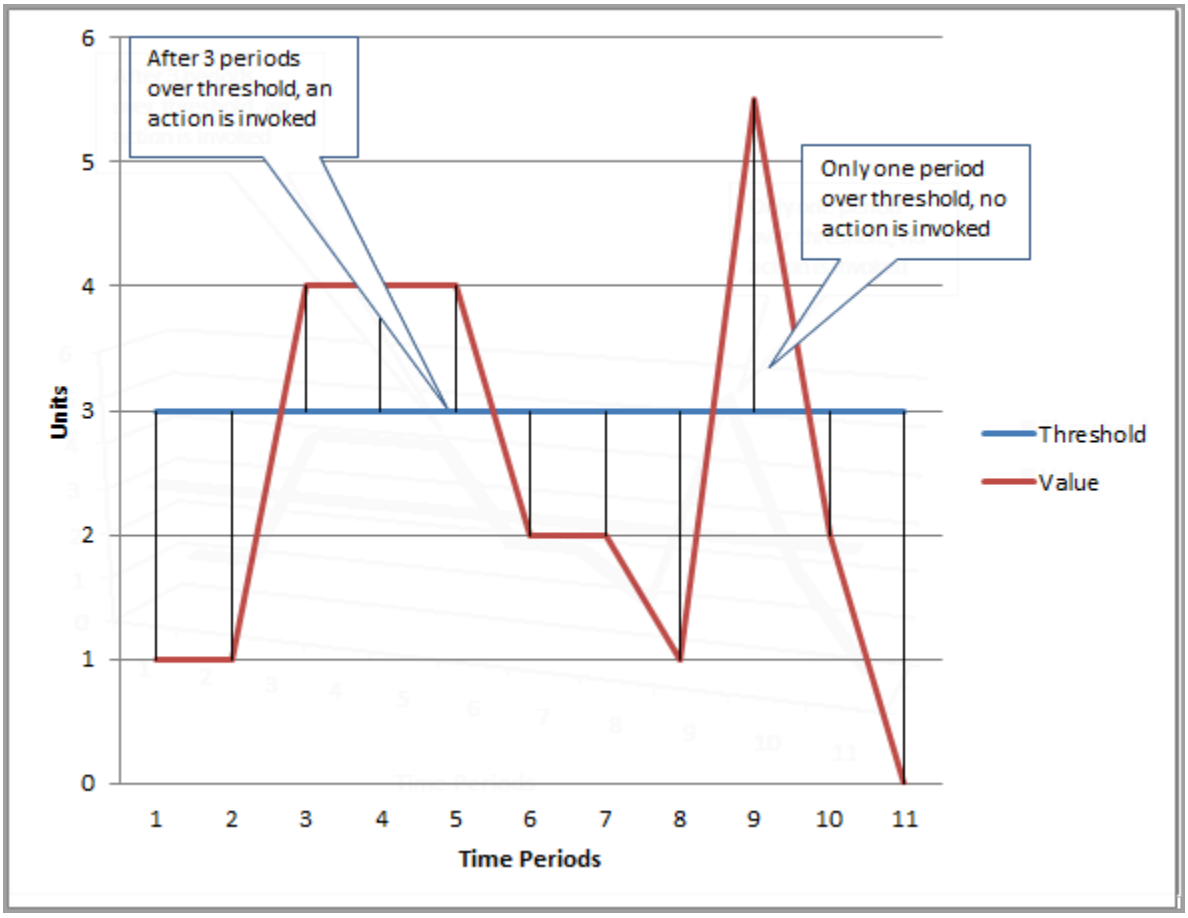
CloudWatch alarmas

Cuando opera las instancias de bases de datos de Amazon RDS, quiere supervisar y generar alertas sobre distintos tipos de métricas, eventos y seguimientos. En el caso de las bases de datos de MySQL y MariaDB, los orígenes de información fundamentales son las métricas de las instancias de base de datos, las métricas del sistema operativo y los eventos, registros y los registros de auditoría. Le recomendamos que utilice CloudWatch las alarmas para observar una única métrica durante el período de tiempo que especifique.

El siguiente ejemplo ilustra cómo puede configurar una alarma que controle la métrica `CPUUtilization` (porcentaje de uso de la CPU) en todas sus instancias de base de datos de Amazon RDS. Puede configurar la alarma para que se active si el uso de la CPU en las instancias de base de datos es superior al 80 % durante el periodo de evaluación de 5 minutos.



Esto significa que la alarma pasa al estado `ALARM` si se hace un uso alto de la CPU de alguna de las bases de datos (más del 80 %) durante 5 minutos o más. La alarma permanece en el estado `OK` si, en algunas ocasiones, la CPU alcanza un nivel de uso superior al 80 % durante un breve periodo y, después, vuelve a caer por debajo del umbral. El siguiente gráfico ilustra este tema.



CloudWatch las alarmas admiten alarmas métricas y compuestas.

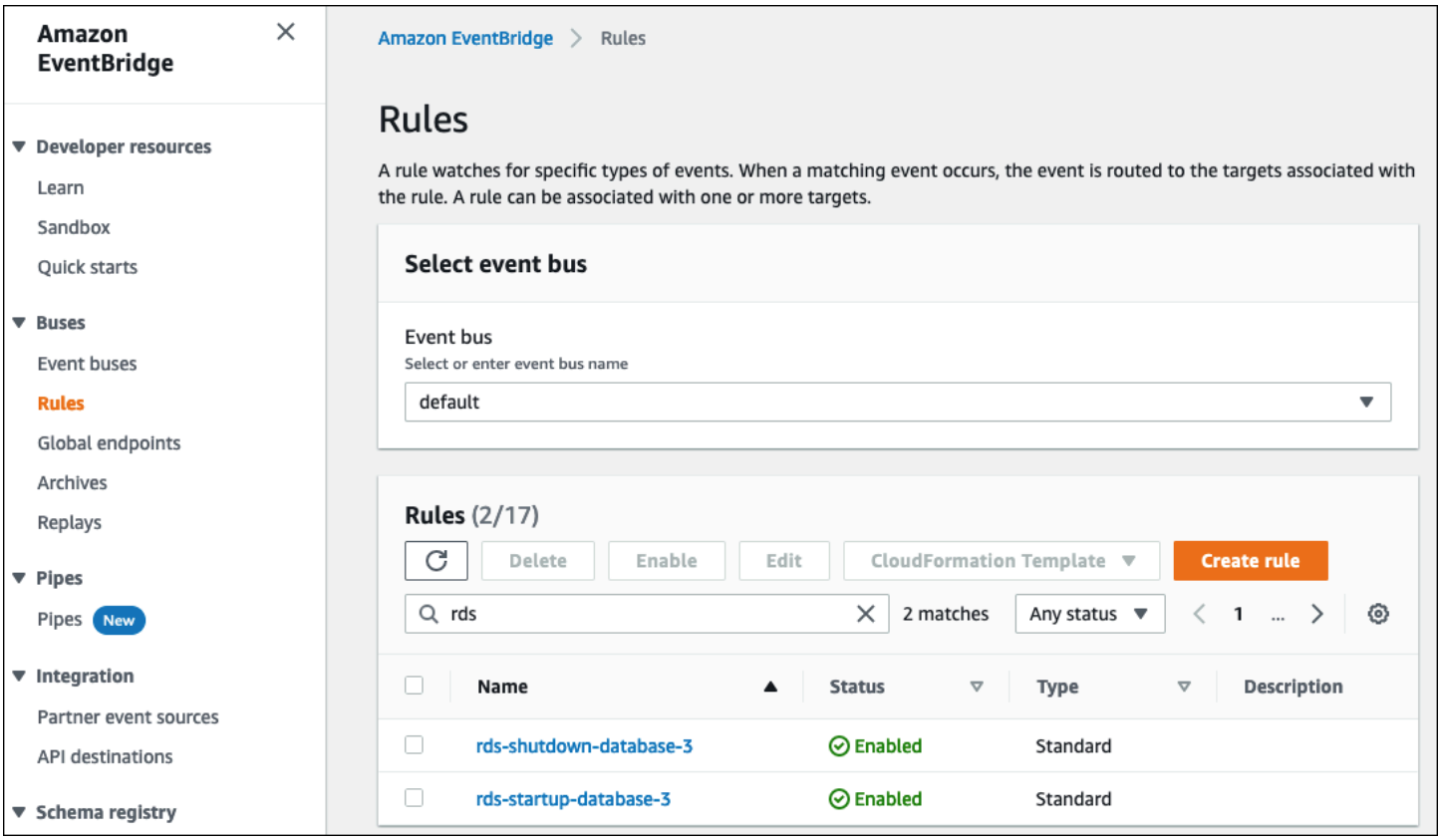
- Una alarma métrica vigila una única CloudWatch métrica y puede realizar expresiones matemáticas en ella. Una alarma de métricas puede enviar mensajes de Amazon SNS que, a su vez, puede tomar una o varias medidas en función del valor de la métrica relativo a un determinado umbral durante una serie de periodos.
- Una alarma compuesta se basa en una expresión de regla, que evalúa los estados de varias alarmas y entra en ese estado `ALARM` solo si se cumplen todas las condiciones de la regla. En general, las alarmas compuestas se utilizan para reducir la cantidad de alertas innecesarias. Por ejemplo, es posible que tenga una alarma compuesta que contenga varias alarmas de métricas configuradas para no tomar ninguna medida. La alarma compuesta enviaría una alerta cuando todas las alarmas de métricas individuales de las compuestas ya estén en el estado `ALARM`

CloudWatch las alarmas solo pueden ver CloudWatch las métricas. Si desea crear una alarma basada en el error, la consulta lenta o los registros generales, debe crear CloudWatch métricas a partir de los registros. Para ello, tal y como se explicó anteriormente en las secciones Supervisión del

sistema operativo y Eventos, registros y registros de auditoría, utilice los filtros para crear métricas a partir de los eventos de registro. Del mismo modo, para alertar sobre las métricas de supervisión mejorada, debe crear filtros de métricas CloudWatch a partir de CloudWatch los registros.

EventBridge reglas

Los eventos de Amazon RDS se envían a Amazon EventBridge y puede utilizar EventBridge reglas para reaccionar ante esos eventos. Por ejemplo, puede crear EventBridge reglas que le notifiquen y tomen medidas si una instancia de base de datos específica se detiene o se inicia, como se muestra en la siguiente pantalla.

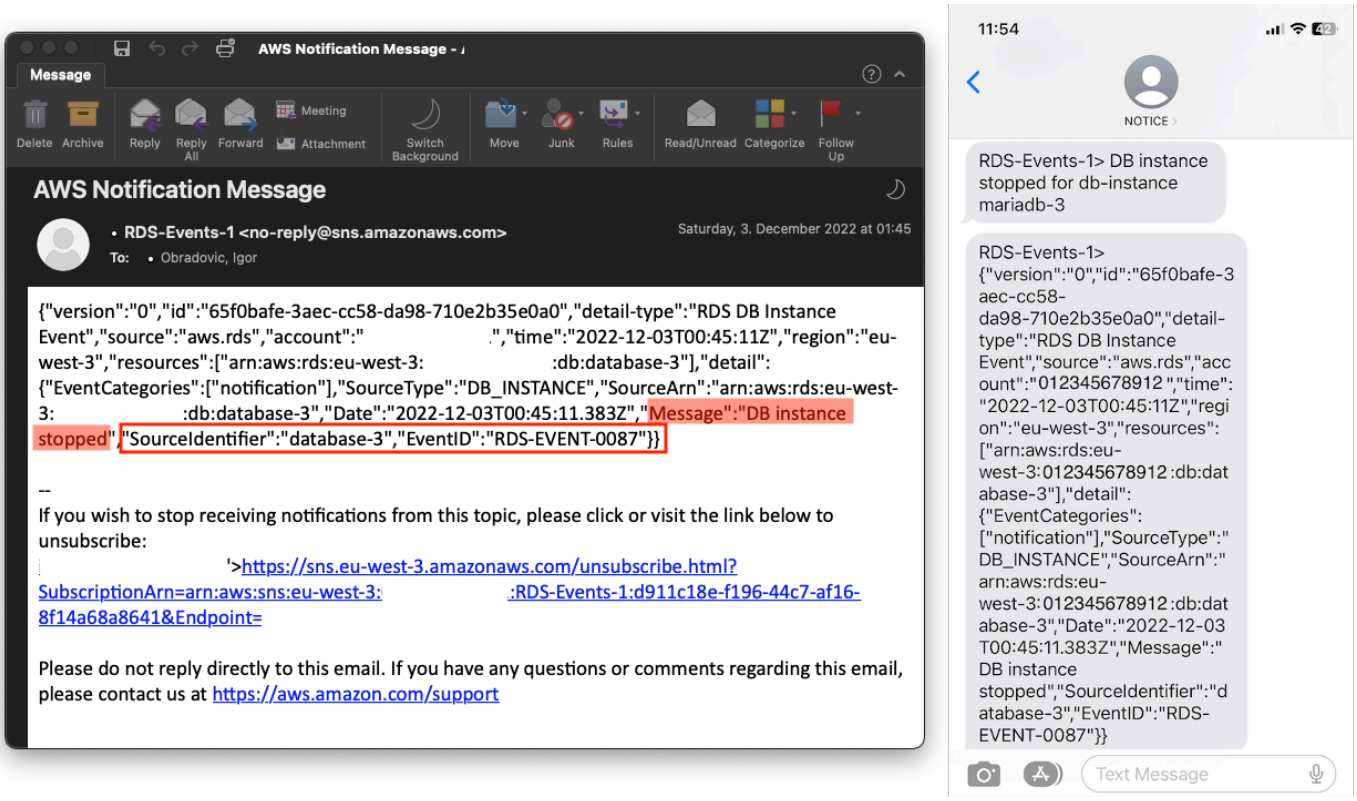


La regla que detecta el evento `The DB instance has been stopped` tiene el id. de evento de Amazon RDS`RDS-EVENT-0087`, por lo que se establece la propiedad `Event Pattern` de la regla en:

```
{
  "source": ["aws.rds"],
  "detail-type": ["RDS DB Instance Event"],
  "detail": {
```

```
    "SourceArn": ["arn:aws:rds:eu-west-3:111122223333:db:database-3"],
    "EventID": ["RDS-EVENT-0087"]
  }
}
```

Esta regla supervisa solo la instancia de base de datos de `database-3` y vigila el evento `RDS-EVENT-0087`. Cuando EventBridge detecta el evento, lo envía a un recurso o punto final, conocido como destino. Aquí puede especificar qué medida desea tomar si la instancia de Amazon RDS se cierra. Puede enviar el evento a muchos destinos posibles, como un tema de SNS, una cola de Amazon Simple Queue Service (Amazon SQS) AWS Lambda , una AWS Systems Manager función, una automatización, un trabajo AWS Batch , Amazon API Gateway y muchos otros. Por ejemplo, puede crear un tema de SNS que envíe una notificación por correo electrónico y un SMS, y asignar ese tema de SNS como destino de la regla. EventBridge Si la instancia de base de datos de Amazon RDS se `database-3` ha detenido, Amazon RDS envía el evento `RDS-EVENT-0087` al EventBridge lugar donde se detecta. EventBridge a continuación, llama al objetivo, que es el tema del SNS. El tema de SNS está configurado para enviar un correo electrónico (como se muestra en la ilustración siguiente) y un SMS.



Especificar las acciones y activar y desactivar las alarmas

Puede usar una CloudWatch alarma para especificar qué acciones debe realizar la alarma cuando cambia entre los estados `OKALARM`, y`INSUFFICIENT_DATA`. CloudWatch tiene una integración integrada con los temas de SNS y varias categorías de acciones adicionales que no son aplicables a las métricas de Amazon RDS, como las acciones de Amazon Elastic Compute Cloud (Amazon EC2) o las acciones grupales de Amazon EC2 Auto Scaling. EventBridge se utiliza generalmente para escribir reglas y definir objetivos que toman medidas cuando se activa la alarma para las métricas de Amazon RDS. CloudWatch envía eventos EventBridge cada vez que una CloudWatch alarma cambia de estado. Puede utilizar estos eventos de cambio de estado de alarma para activar un objetivo de evento EventBridge. Para obtener más información, consulte los eventos de alarma y EventBridge la CloudWatch documentación.

Es posible que también deba administrar las alarmas. Por ejemplo, desactivar automáticamente una alarma durante las pruebas o los cambios de configuración planificados y, a continuación, volver a activarla cuando finalice la medida planificada. Por ejemplo, si tiene una actualización planificada y programada del software de la base de datos que requiere tiempo de inactividad y tiene alarmas que se activarán si la base de datos deja de estar disponible, puede deshabilitar y activar las alarmas mediante las acciones DisableAlarmActionsde la API o enable-alarm-actionslos comandos disable-alarm-actionsy del AWS CLI. EnableAlarmActions También puede ver el historial de alarmas en la CloudWatch consola o mediante la acción de la DescribeAlarmHistoryAPI o el describe-alarm-historycomando del AWS CLI. CloudWatch conserva el historial de alarmas durante dos semanas. En la CloudWatch consola, puede seleccionar el menú Favoritos y recientes del panel de navegación para configurar sus alarmas favoritas y las que ha visitado más recientemente y acceder a ellas.

Próximos pasos y recursos

Para más información sobre la migración de las bases de datos relacionales a Nube de AWS, consulte la siguiente estrategia en el sitio web de recomendaciones de AWS:

- Estrategia de migración para bases de datos relacionales

Puede explorar los patrones de migración de las bases de datos de las recomendaciones de AWS para obtener instrucciones detalladas de las bases de datos relacionales concretas que se ejecutan en Nube de AWS, lo que incluye las tareas relacionadas con la supervisión, la migración y la gestión de datos.

Para obtener más ayuda, consulte los siguientes recursos:

- Guía de usuario de Amazon Relational Database Service
- Guía del usuario de Amazon CloudWatch
- Preguntas frecuentes de Amazon RDS
- Preguntas frecuentes de Información de rendimiento
- Envíe las métricas de contadores de Información de rendimiento de Amazon RDS a un proveedor de servicios de supervisión del rendimiento de aplicaciones externo mediante Flujo de métricas de Amazon CloudWatch (entrada del blog de AWS)
- Creación de un panel de Amazon CloudWatch para supervisar Amazon RDS y Amazon Aurora MySQL (entrada del blog de AWS)
- Ajuste de Amazon RDS para MySQL con Información de rendimiento (entrada del blog de AWS)

Historial de documentos

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

Cambio	Descripción	Fecha
Información actualizada sobre Información de rendimiento	Se actualizó la sección acerca de la publicación de métricas de Información de rendimiento en CloudWatch con la información más reciente.	11 de marzo de 2025
Se actualizó la información acerca de los exportadores	Se actualizó la información acerca de los exportadores y se agregaron recomendaciones para elegir un exportador.	13 de junio de 2024
Publicación inicial	—	30 de junio de 2023

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.

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.