



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

AWS Guía prescriptiva



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

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Introducción	1
Descripción general	3
Resultados empresariales específicos	4
Prácticas recomendadas generales	7
Herramientas de supervisión	9
Herramientas incluidas en Amazon RDS	10
CloudWatch espacios de nombres	10
CloudWatch alarmas y paneles	12
Información de rendimiento de Amazon RDS	13
Supervisión mejorada	15
Servicios adicionales AWS	15
Herramientas de monitoreo de terceros	17
Prometheus y Grafana	17
Percona	19
Supervisión de instancias de base de datos	20
Métricas de Performance Insights para instancias de bases de datos	21
Carga de base de datos	21
Dimensiones	22
Métricas de contador	23
Estadísticas de SQL	26
CloudWatch métricas para instancias de bases de datos	27
Publicar métricas de Performance Insights en CloudWatch	28
Supervisión del sistema operativo	30
Eventos, registros y pistas de auditoría	37
Eventos de Amazon RDS	37
Registros de la base de datos	41
Registros de seguimiento de auditoría	44
Ejemplo	45
Funciones adicionales CloudTrail y CloudWatch de registro	48
Alertas	50
CloudWatch alarmas	51
EventBridge reglas	54
Especificar acciones y habilitar y deshabilitar las alarmas	56
Próximos pasos y recursos	57

Historial de documentos	58
Glosario	59
#	59
A	60
B	63
C	65
D	68
E	73
F	75
G	77
H	78
I	80
L	82
M	83
O	88
P	91
Q	94
R	94
S	97
T	101
U	103
V	103
W	104
Z	105
.....	cvi

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

Igor Obradovic, Amazon Web Services (AWS)

Marzo de 2025 (historia [del documento](#))

El monitoreo de una base de datos es el proceso de medir, rastrear y evaluar la disponibilidad, el rendimiento y la funcionalidad de una base de datos. Las soluciones de monitoreo y alerta 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, resilientes y eficientes. Además 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 sus recursos para asegurarse de que funcionan según lo esperado y para detectar y solucionar cualquier problema antes de que afecte a sus clientes. Debe utilizar las métricas, los registros, los eventos y los seguimientos que supervisa para generar alarmas cuando se superen los umbrales.

Esta guía describe las herramientas de supervisión y observabilidad de 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 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. Nube de AWS

Contenido

- [Información general](#)
- [Prácticas recomendadas generales](#)
- [Herramientas de supervisión](#)
- [Supervisión de instancias de base de datos](#)
- [Supervisión del sistema operativo](#)

- [Eventos, registros y registros de auditoría](#)
- [Alertas](#)
- [Próximos pasos y recursos](#)

Descripción general

La supervisión y las alertas se incluyen en cuatro pilares del [AWS Well-Architected Framework](#).

- El [pilar de la excelencia operativa](#) establece que la carga de trabajo debe diseñarse de manera que incluya la telemetría y la supervisión. AWS servicios como [Amazon Relational Database Service \(Amazon RDS\)](#) proporcionan la información necesaria para que comprenda el estado interno de su carga de trabajo (por ejemplo, métricas, registros, eventos y seguimientos). Cuando utilice sus bases de datos de Amazon RDS, querrá comprender el estado de las instancias de sus bases de datos, detectar eventos operativos y poder responder a eventos planificados y no planificados. AWS proporciona herramientas de monitoreo que le ayudan a determinar cuándo los resultados de la organización y el negocio están en riesgo o podrían estar en riesgo, 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 sus 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 causaron (por ejemplo, consultas SQL no optimizadas o parámetros de configuración inadecuados). Puede activar las alarmas automáticamente cuando las mediciones estén fuera de los límites esperados. Le recomendamos que utilice 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 comparándolas con umbrales predefinidos o utilizar algoritmos de aprendizaje automático para identificar un comportamiento anómalo. Por ejemplo, para detectar una tendencia de aumento del uso de la CPU, puede recopilar y analizar la `cpuUtilization.total` métrica durante un período de tiempo. Alertar sobre esa anomalía de forma proactiva, antes de que el uso de la CPU alcance el límite máximo, puede ayudarle a solucionar el problema antes de que afecte a sus clientes.
- El [pilar de la fiabilidad](#) define la supervisión y las alertas como fundamentales para garantizar que se cumplen los requisitos de disponibilidad. Su solución de monitorización debe poder detectar los fallos de forma eficaz. Cuando detecta problemas o fallos, su objetivo principal es alertar sobre esos problemas. La implementación de prácticas continuas de observabilidad y monitoreo es imprescindible para las arquitecturas resilientes en la nube. Para mejorar sus cargas de trabajo, debe poder medirlas y comprender su estado y estado. Los principios de diseño para la recuperación automática en caso de fallo, 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 la prevención de cambios de configuración inesperados o no deseados y de comportamientos inesperados. Puede configurar sus instancias de base de datos de Amazon RDS for MySQL y MariaDB con el complemento de [auditoría MariaDB para registrar la actividad de la base de datos, como los inicios de sesión](#) de los usuarios y las operaciones específicas 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 monitoreo y alerta. El archivo de registro se analiza en tiempo real para detectar comportamientos inesperados o sospechosos en la base de datos. Este comportamiento inesperado o sospechoso puede indicar que su instancia de base de datos de Amazon RDS se ha visto comprometida, lo que indica posibles riesgos para su empresa. Si la herramienta de monitoreo 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 las mejores prácticas en los mecanismos de monitoreo y alerta le ayuda a garantizar una infraestructura de alto rendimiento, resiliente, eficiente, segura y rentable para sus aplicaciones y cargas de trabajo. Puede utilizar herramientas de observabilidad que recopilan, almacenan y visualizan métricas, eventos, trazas y registros en tiempo real para observar y analizar el panorama general del estado y el rendimiento de sus bases de datos y, de este modo, evitar la degradación o la interrupción de los servicios de TI asociados. Si aún se produce una degradación imprevista o una interrupción del servicio, las herramientas de supervisión y alerta le ayudan a detectar el problema a tiempo, a intensificarlo y reaccionar, y a investigar y resolver rápidamente. Una solución integral de monitoreo y alertas para las cargas de trabajo de sus bases de datos en la nube le ayuda a lograr los siguientes resultados empresariales:

- **Mejore la experiencia del cliente.** Un servicio fiable mejora la experiencia de sus clientes. Las bases de datos suelen ser un componente clave de los servicios digitales, como las aplicaciones web y móviles, la transmisión multimedia, los pagos business-to-business (B2B) APIs y los servicios de integración. Si puede monitorear y configurar alertas en sus bases de datos para detectar problemas rápidamente, 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 sus clientes.
- **Genere la confianza de los clientes.** Un mejor rendimiento y una experiencia de usuario más fluida le ayudan a ganarse la confianza de sus 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 en línea confiable puede esperar una alta confianza y fidelidad de los clientes, 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. Cualquier tiempo de inactividad inesperado en la infraestructura de su base de datos puede afectar a las transacciones comerciales que sus clientes realizan con su aplicación. En algunos casos, esto puede provocar pérdidas financieras sustanciales. El incumplimiento de los acuerdos de nivel de servicio (SLAs) puede provocar la pérdida de la confianza de los clientes y, en consecuencia, la pérdida de ingresos. También puede convertirse en una base legal para juicios costosos, en los que los clientes pueden exigir una compensación en función de sus contratos de responsabilidad y garantía. Según un [estudio realizado por Atlassian Corporation](#), una empresa de software, los costes medios de una interrupción del servicio oscilan entre 140 000 y 540 000 dólares por hora, según el tipo y el tamaño de la empresa. Un entorno de base de datos estable es fundamental para evitar interrupciones prolongadas y pérdidas de negocio.
- Amplíe el valor. Los mecanismos de monitoreo y alerta pueden ayudarlo a 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 en la nube existentes e introduzca nuevos servicios. Los nuevos servicios proporcionan un valor adicional a sus clientes y más ingresos a su empresa, lo que repercute en su crecimiento.
- Mejore la productividad de los desarrolladores. Los desarrolladores que son 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, y 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 trazas correlacionadas. Estas 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 monitoreo y alerta puede ayudar a los desarrolladores a programar y probar mejor y más rápido.
- Mejore la eficacia y la eficiencia operativas. Al operar 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 monitorear sus bases de datos y analizar las métricas, los eventos, los registros y los rastreos, puede comprender y predecir sus necesidades de capacidad futuras y aprovechar los

ahorros de costos disponibles en el Nube de AWS. Comprender las cargas de trabajo y el estado operativo de Amazon RDS puede ayudarle a responder a los eventos, solucionar problemas y planificar mejoras.

Prácticas recomendadas generales

Las siguientes prácticas recomendadas le ayudan a obtener una visibilidad suficiente del estado de su carga de trabajo de Amazon RDS y a tomar las medidas adecuadas en respuesta a los eventos operativos y los datos de monitoreo.

- **Identifique KPIs.** Identifique los indicadores clave de rendimiento (KPIs) en función de los resultados empresariales deseados. Evalúe KPIs para determinar el éxito 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 las 24 horas del día, los 7 días de la semana, para que sus clientes puedan hacer sus compras. 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 referencia en el 99,99% semanalmente. La evaluación del KPI de disponibilidad real con respecto al valor de referencia le ayuda a determinar si está cumpliendo 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 métricas de carga de trabajo para medir las cantidades y calidades de su carga de trabajo de Amazon RDS. Evalúe las métricas para determinar si la carga de trabajo está logrando los resultados deseados y para comprender el estado de la carga de trabajo. Por ejemplo, para evaluar el KPI de disponibilidad de su instancia de base de datos de Amazon RDS, debe medir métricas como el tiempo de actividad y el tiempo de inactividad de la instancia de base de datos. A continuación, puede usar 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, que son útiles en la categorización y el análisis.

- **Recopile y analice las métricas de carga de trabajo.** Amazon RDS genera diferentes métricas y registros, en función de la configuración. Algunos de ellos representan eventos, contadores o estadísticas de la instancia de base de datos, por ejemplo, `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 anfitriona de Amazon Elastic Compute Cloud (Amazon EC2). La herramienta de monitoreo debe realizar

un análisis periódico y proactivo de las métricas recopiladas para identificar las tendencias y determinar si se necesitan respuestas adecuadas.

- Establezca bases de referencia para las métricas de carga de trabajo. Establezca bases de referencia para las métricas a fin de definir los valores esperados e identificar los umbrales buenos o incorrectos. Por ejemplo, puede definir la línea base para ReadIOPS que sea de hasta 1000 en operaciones normales de base de datos. A continuación, puede utilizar esta línea base para comparar e identificar la sobreutilización. Si sus nuevas métricas muestran consistentemente que las IOPS leídas oscilan entre 2000 y 3000, habrá identificado una desviación que podría provocar una respuesta que permitiera investigar, intervenir y mejorar.
- Alerta 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 sus clientes, o mitigar el impacto del incidente de manera oportuna.
- Identifique los patrones de actividad esperados para su carga de trabajo. En función de las métricas de referencia, establezca patrones de 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 aprendizaje automático para analizar las métricas y detectar anomalías.
- Alerta cuando se detecten anomalías en la carga de trabajo. Cuando se detecten anomalías en las operaciones de las cargas de trabajo de Amazon RDS, emita una alerta para que pueda responder con las acciones adecuadas si es necesario.
- Revise y revise las métricas. KPIs Confirme que sus 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 evaluadas KPIs, y revíselas si es necesario. Por ejemplo, supongamos que establece un KPI para el número óptimo de conexiones simultáneas a bases de datos y supervisa las métricas relacionadas con las conexiones intentadas y fallidas, así como los hilos de usuario que se crearon y están en ejecución. Es posible que tenga más conexiones a bases de datos que las definidas en el KPI de referencia. Al analizar las métricas actuales, puede detectar el resultado, pero es posible que no pueda determinar la causa raíz. Si es así, debería revisar tus métricas e incluir medidas de supervisión adicionales, como contadores para bloquear las mesas. 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 que utilice herramientas de observabilidad, monitoreo y alertas para:

- Obtenga información sobre el rendimiento de su entorno 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 sus usuarios se vean afectados

Puede elegir entre diferentes opciones y soluciones, entre las que se incluyen herramientas y servicios de monitoreo y observabilidad nativos de la nube AWS proporcionados; soluciones de software gratuitas y de código abierto; y soluciones comerciales de terceros para monitorear las instancias de bases de datos de Amazon RDS. Algunas de estas herramientas se describen en las secciones siguientes.

Para determinar qué herramienta se adapta mejor a sus necesidades, compare las características y capacidades de cada herramienta con los requisitos de su organización. También le recomendamos que evalúe las herramientas para determinar la facilidad de despliegue, 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 cualquier otro factor que sea específico de su organización.

Secciones

- [Herramientas incluidas en Amazon RDS](#)
- [CloudWatch espacios de nombres](#)
- [CloudWatch alarmas y paneles](#)
- [Amazon RDS Performance Insights](#)
- [Supervisión mejorada](#)
- [Servicios adicionales AWS](#)
- [Herramientas de monitoreo de terceros](#)

Herramientas incluidas en Amazon RDS

Amazon Relational Database Service (Amazon RDS) es un servicio de base de datos gestionado en Nube de AWS. Como Amazon RDS es un servicio gestionado, 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 parches del sistema operativo y del 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 que le permiten crear una solución de [observabilidad](#) completa para sus instancias de base de datos de Amazon RDS.

Algunas de las herramientas de supervisión están incluidas, preconfiguradas y habilitadas automáticamente en el servicio Amazon RDS. En cuanto inicie su 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 base de datos. Por ejemplo, los códigos de estado incluyen Disponible, Detenida, Creando, Backing-up y Fallada. 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 obtener más información, consulte [Visualización del estado de la instancia de base de datos de Amazon RDS](#) en la documentación de Amazon RDS.
- Las recomendaciones de Amazon RDS proporcionan recomendaciones automatizadas para instancias de base de datos, réplicas de lectura y grupos de parámetros de base de datos. Estas recomendaciones se proporcionan mediante el análisis del uso, los datos de rendimiento y la configuración de las instancias de base de datos, y se proporcionan a modo de orientación. Por ejemplo, la recomendación de que la versión del motor esté desactualizada sugiere que sus instancias de base de datos no ejecutan la última versión del software de base de datos y que debería actualizarla para beneficiarse de las últimas correcciones de seguridad y otras mejoras. Para obtener más información, consulte [Visualización de las recomendaciones de Amazon RDS](#) en la documentación de Amazon RDS.

CloudWatch espacios de nombres

Amazon RDS se integra con [Amazon CloudWatch](#), que es un servicio de supervisión y alertas para los recursos y aplicaciones de la nube que se ejecutan en ella. AWS Amazon RDS recopila automáticamente métricas, archivos de registro, seguimientos y eventos sobre el funcionamiento, la

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

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

- El espacio de [nombres de AWS/RDS incluye métricas a nivel](#) de instancia 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) y muchos más.
- [El espacio de nombres AWS/Usage incluye métricas de uso a nivel de cuenta, que se utilizan para determinar si está operando dentro de las cuotas de servicio de Amazon RDS.](#) Los ejemplos 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 AWS cuenta o región) y `ManualSnapshots` (el número de instantáneas de bases de datos creadas manualmente en su AWS cuenta o región).

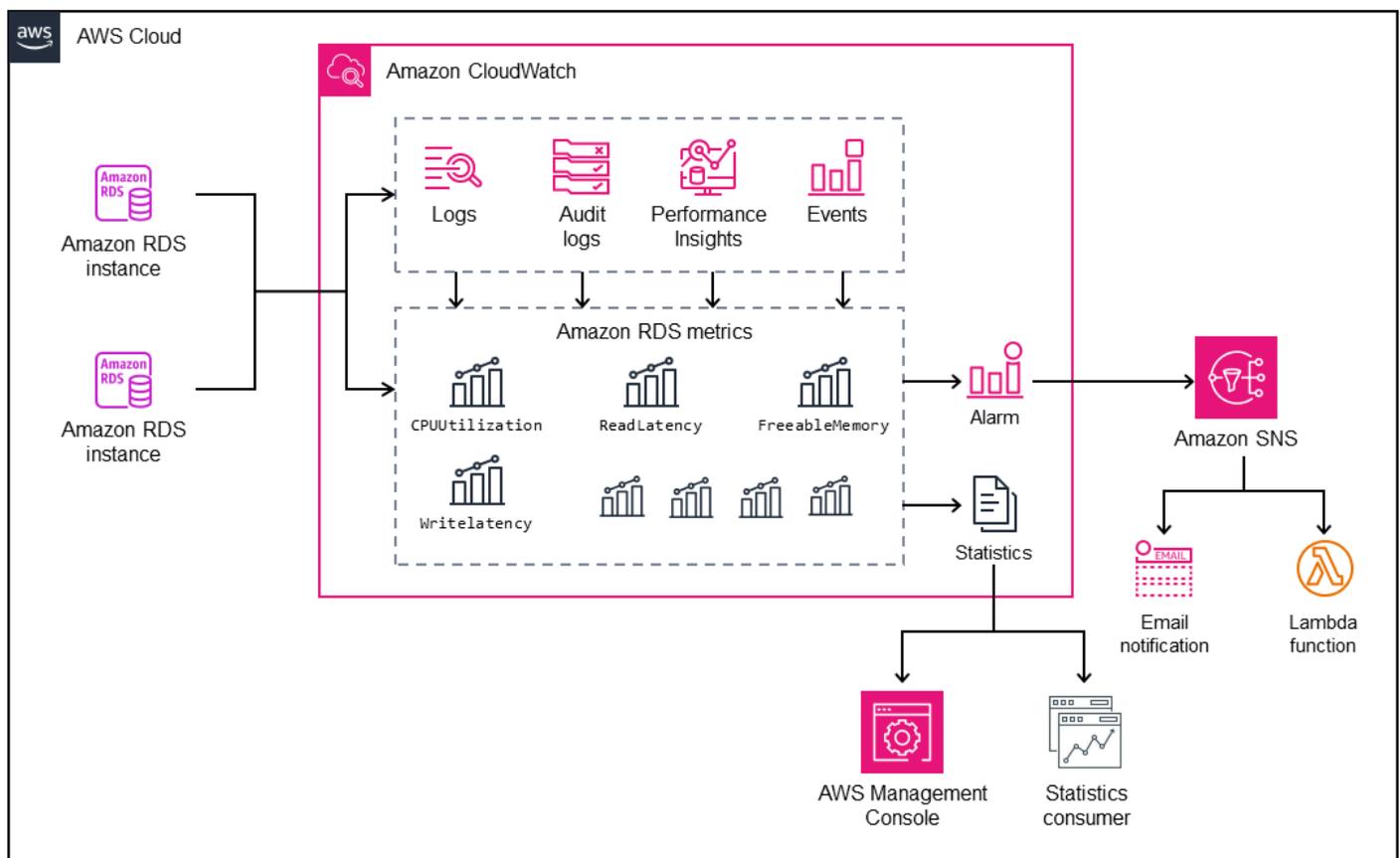
CloudWatch conserva los datos métricos de la siguiente manera:

- 3 horas: las métricas personalizadas de alta resolución con un período inferior a 60 segundos se conservan durante 3 horas. Transcurridas 3 horas, los puntos de datos se agregan en métricas de períodos de 1 minuto y se conservan durante 15 días.
- 15 días: los puntos de datos con un período de 60 segundos (1 minuto) se conservan durante 15 días. Después de 15 días, los puntos de datos se agregan en métricas de períodos de 5 minutos y se conservan durante 63 días.
- 63 días: los puntos de datos con un período de 300 segundos (5 minutos) se conservan durante 63 días. Después de 63 días, los puntos de datos se agregan en métricas de un período de 1 hora y se conservan durante 15 meses.
- 15 meses: los puntos de datos con un período de 3.600 segundos (1 hora) están disponibles durante 15 meses (455 días).

Para obtener más información, consulte [Métricas](#) en la CloudWatch documentación.

CloudWatch alarmas y paneles

Puede utilizar [CloudWatch las alarmas de Amazon](#) para ver una métrica específica de Amazon RDS durante un período de tiempo. Por ejemplo, puede supervisar `FreeStorageSpace`, a continuación, realizar una o más acciones si el valor de la métrica supera el umbral que haya 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 automáticamente almacenamiento adicional para la instancia de base de datos de Amazon RDS. La alarma también puede enviar un SMS de notificación al DBA mediante Amazon Simple Notification Service (Amazon SNS). En el siguiente diagrama se ilustra este proceso.



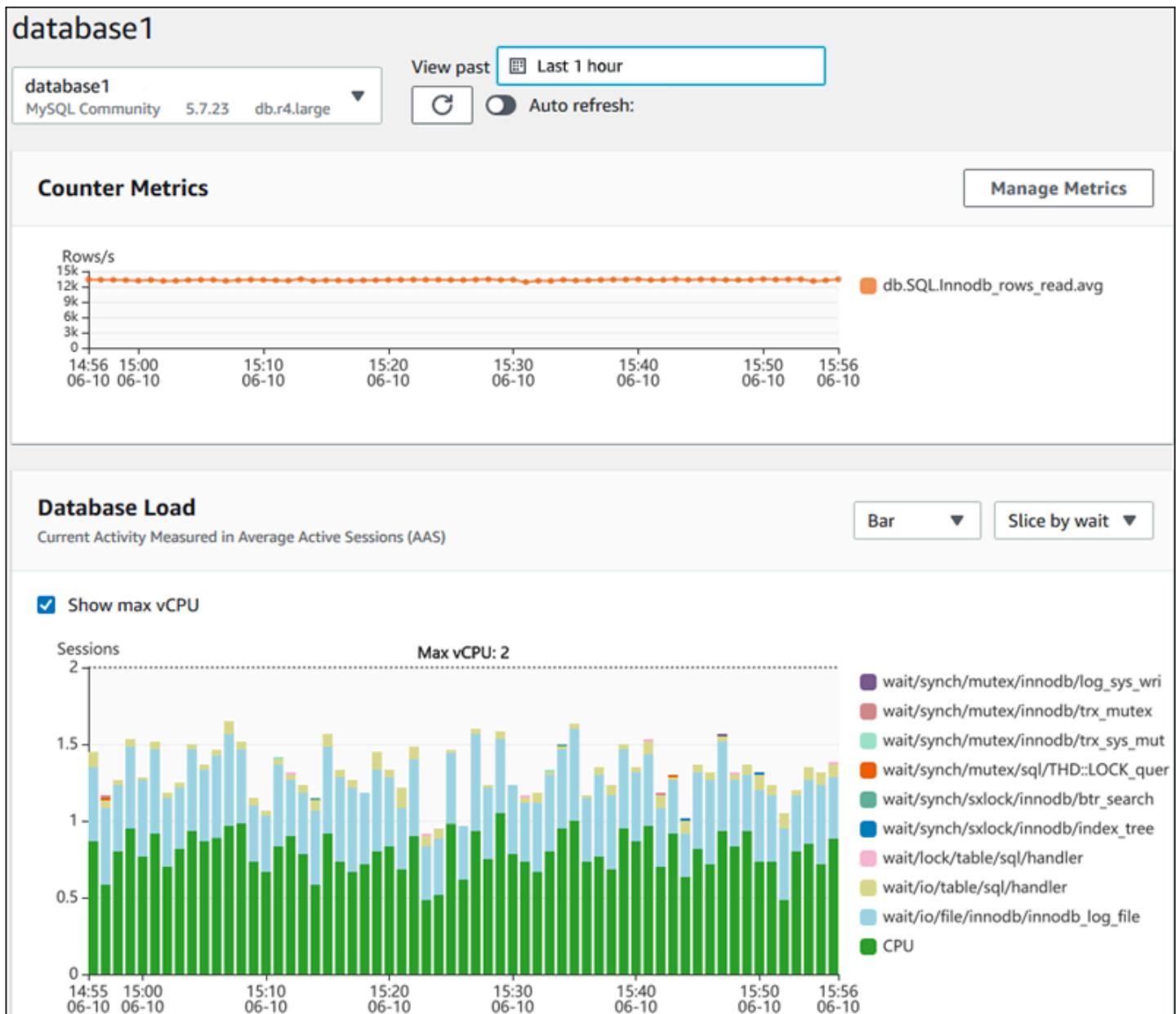
CloudWatch también proporciona [paneles](#), que puede utilizar para crear, personalizar, interactuar y guardar vistas personalizadas (gráficos) de las métricas. También puede utilizar [CloudWatch Logs Insights](#) para crear un panel de control que permita supervisar el registro de consultas lento y el registro de errores y recibir alertas si se detecta un patrón específico en esos registros. En la siguiente pantalla se muestra un CloudWatch panel de ejemplo.

The screenshot displays the Amazon RDS Performance Insights dashboard for a MySQL instance. It is divided into several sections:

- Slow queries with detailed info:** A table listing the top slowest queries. Columns include Rank, Time, User, Id, Query_time, Lock_time, Rows_sent, Rows_examined, timestamp, and query. The top query is a SELECT statement with a complex JOIN.
- Top Slow Queries sorted by Query Time:** A table showing the top slowest queries with columns for Rank, Time, Query_time, and Query. The top query is a SELECT COUNT(*) statement.
- Top 200 lines of Error Log:** A list of error messages with columns for Rank, Message, and details. The top error is a connection error: "ready for connections. Version: '5.7.12-log' socket: '/tmp/mysql.sock' port: 3306 MySQL Comm."

Información de rendimiento de Amazon RDS

[Amazon RDS Performance Insights](#) es una herramienta de supervisión y ajuste del rendimiento de las bases de datos que amplía las funciones de supervisión de Amazon RDS. Le ayuda a analizar el rendimiento de la base de datos visualizando la carga de la instancia de base de datos y filtrándola por esperas, sentencias SQL, hosts o usuarios. La herramienta combina varias métricas en un único gráfico interactivo que le ayuda a identificar el tipo de obstáculo que puede tener su instancia de base de datos, como las esperas bloqueadas, el alto consumo de CPU o la latencia de E/S, y a determinar qué sentencias SQL están creando el cuello de botella. La siguiente pantalla muestra un ejemplo de visualización.



Debe [habilitar Performance Insights](#) 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 su cuenta. La capa gratuita incluye siete días de historial de datos de rendimiento y un millón de solicitudes de API al mes. Si lo desea, puede adquirir períodos de retención más largos. Para obtener información completa sobre los precios, consulte los [precios de Performance Insights](#).

Para obtener información sobre cómo puede usar Performance Insights para monitorear sus instancias de base de datos, consulte la sección de [monitoreo de instancias de base](#) de datos más adelante en esta guía.

Performance Insights [publica automáticamente las métricas en CloudWatch](#). Además de utilizar la herramienta Performance Insights, puede aprovechar las funciones adicionales que CloudWatch ofrece. Puede examinar las métricas de Performance Insights mediante la CloudWatch consola AWS CLI, la o la CloudWatch API. También puede añadir CloudWatch alarmas, como con cualquier otra métrica. Por ejemplo, es posible que desees activar una notificación por SMS DBAs o tomar una medida correctiva si la DBLoad métrica supera el valor límite que has establecido. También puede añadir las métricas de Performance Insights a sus CloudWatch paneles existentes.

Supervisión mejorada

La [monitorización mejorada](#) es una herramienta que captura las métricas en tiempo real del 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 OS, 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 Performance Insights, Amazon RDS entrega las métricas de Enhanced Monitoring a CloudWatch, donde puede beneficiarse de funciones adicionales, como la conservación a largo plazo de las métricas para su análisis, la creación de filtros de métricas, la visualización de gráficos en el CloudWatch panel de control y la configuración de alarmas. De forma predeterminada, la monitorización mejorada está deshabilitada al crear una nueva instancia de base de datos de Amazon RDS. Puede [habilitar](#) la función al crear o modificar una instancia de base de datos. El precio se basa en la cantidad de datos transferidos de Amazon RDS a CloudWatch Logs y en las tarifas de almacenamiento. En función de la granularidad y del número de instancias de base de datos en las que esté habilitada la monitorización mejorada, parte de los datos de monitorización se puede incluir en la capa gratuita de CloudWatch Logs. Para obtener información completa sobre los precios, consulta [Amazon CloudWatch Pricing](#). Para obtener más información sobre la herramienta, consulte la [documentación de Amazon RDS](#) y las preguntas frecuentes sobre la [monitorización mejorada](#).

Servicios adicionales AWS

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

- [Amazon EventBridge](#) es un bus de eventos sin servidor que puede recibir, filtrar, transformar, enrutar y entregar eventos desde sus aplicaciones y AWS recursos, incluidas sus 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 entrega eventos a CloudWatch Events y EventBridge prácticamente en tiempo real. Con EventBridge and CloudWatch Events, puede definir reglas para enviar alertas sobre eventos específicos de Amazon RDS de interés y automatizar las acciones que se llevarán a cabo cuando un evento coincida con la regla. Hay una variedad de objetivos disponibles en respuesta a un evento, como una AWS Lambda función que puede realizar una acción correctiva o un tema de Amazon SNS que puede enviar un correo electrónico o un SMS para notificar DBAs el evento a DevOps nuestros ingenieros.

- [Amazon CloudWatch Logs](#) es un servicio que centraliza el almacenamiento de los archivos de registro de todas sus aplicaciones, sistemas y AWS servicios, incluidas las instancias de bases de datos Amazon RDS for MySQL y MariaDB y. AWS CloudTrail Si [habilita](#) la función para sus instancias de base de datos, Amazon RDS publica automáticamente los siguientes registros en CloudWatch Logs:

- Registro de errores
- Registro de consultas lentas
- Registro general
- Registro de auditoría

Puede utilizar CloudWatch Logs Insights para consultar y analizar los datos de registro. La función incluye un lenguaje de consulta especialmente diseñado que le ayuda a buscar eventos de registro que coincidan con los patrones que usted defina. Por ejemplo, puede realizar un seguimiento de los daños en las tablas de su instancia de base de datos MySQL supervisando el siguiente patrón en el archivo de registro de errores: `"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 CloudWatch métricas. A continuación, puede usar las métricas para crear paneles con gráficos o datos tabulares, o configurar una alarma si se supera el valor umbral definido. Esto resulta especialmente útil cuando se utiliza el registro de auditoría, ya que puede supervisar automáticamente, enviar alertas y tomar medidas correctivas si se detecta algún comportamiento inesperado o sospechoso. Puede acceder a los registros de la base de datos y gestionarlos mediante la consola de AWS administración AWS CLI, la API de Amazon RDS o el AWS SDK for CloudWatch Logs.

- [AWS CloudTrail](#) registra y supervisa de forma continua la actividad de los usuarios y las API en su Cuenta de AWS. Le ayuda a auditar, supervisar la seguridad y solucionar problemas operativos de sus instancias de base de datos Amazon RDS for MySQL o MariaDB. CloudTrail está integrado

con Amazon RDS. Todas las acciones se pueden registrar y CloudTrail proporciona un registro de las acciones realizadas por un usuario, rol o AWS servicio 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 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. Los eventos que se registran CloudTrail incluyen tanto las llamadas desde la consola de Amazon RDS como las llamadas desde el código que usa la API de Amazon RDS.

Herramientas de monitoreo de terceros

En algunos escenarios, además del conjunto completo de herramientas de monitoreo y observabilidad nativas de la nube que AWS proporciona Amazon RDS, es posible que desee utilizar herramientas de monitoreo de otros proveedores de software. Estos escenarios incluyen las implementaciones híbridas, en las que puede tener varias bases de datos ejecutándose en su centro de datos local y otro conjunto de bases de datos ejecutándose en el. Nube de AWS Si ya ha establecido su solución de observabilidad corporativa, es posible que desee seguir utilizando las herramientas existentes y ampliarlas a sus implementaciones. Nube de AWS El desafío de configurar una solución de monitoreo de terceros suele residir en las salvaguardas que impone Amazon RDS como servicio gestionado en la nube. Por ejemplo, no puede instalar el software de agente en el sistema operativo anfitrión 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 monitoreo de terceros con Amazon RDS basándose en CloudWatch otros Nube de AWS servicios. Por ejemplo, las métricas, los registros, los eventos y las trazas de Amazon RDS se pueden exportar y, a continuación, importar a la herramienta de monitoreo de terceros para su posterior análisis, visualización y alertas. Algunas de estas soluciones de terceros incluyen Prometheus, Grafana y Percona.

Prometheus y Grafana

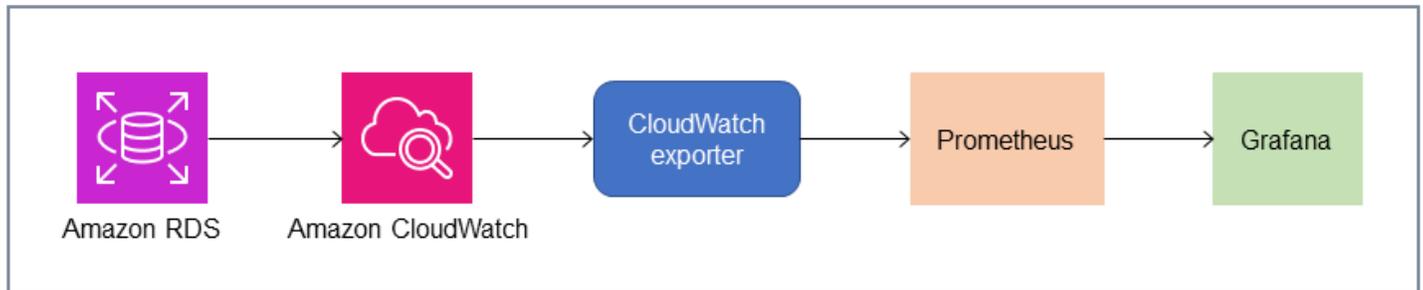
[Prometheus](#) es [una](#) solución de monitoreo de código abierto que recopila métricas de objetivos configurados a intervalos determinados. Es una solución de monitoreo de uso general que puede monitorear cualquier aplicación o servicio. Cuando supervisa las instancias de base de datos de Amazon RDS, CloudWatch recopila las métricas de Amazon RDS. Luego, las métricas se exportan

al servidor Prometheus mediante un exportador de código abierto, como YACE Exporter o Exporter. CloudWatch

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

Al elegir un exportador, diseñar el modelo de despliegue y configurar las instancias del exportador, tenga en cuenta [CloudWatchy](#) [CloudWatch registre](#) las cuotas de servicio y API, ya que la exportación de CloudWatch métricas a un servidor Prometheus se implementa sobre la API. CloudWatch Por ejemplo, la implementación de varias instancias de CloudWatch Exporter en una sola región Cuenta de AWS y para monitorear cientos de instancias de base de datos de Amazon RDS podría provocar 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, debería 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 exportadoras en cada una. Cuenta de AWS

[Las alertas son generadas por el servidor Prometheus y gestionadas por Alertmanager](#). 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 funciones de análisis, como consultas ad hoc y desglose dinámico. También puede buscar y analizar registros, e incluye funciones de alerta para evaluar continuamente 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 monitoreo, 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 funciones adicionales, 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, INFORMATION_SCHEMA consulta las estadísticas del servidor, el esquema del sistema y el esquema de rendimiento, y utiliza la CloudWatch API para adquirir métricas, registros, eventos y seguimientos. PMM requiere una clave de acceso de usuario AWS Identity and Access Management (IAM) (función de IAM) y descubre automáticamente las instancias de base de datos de Amazon RDS que están disponibles para su supervisión. La herramienta PMM está perfilada para el monitoreo de bases de datos y recopila más métricas específicas de bases de datos que Prometheus. Para usar el [panel de análisis de consultas de PMM](#), debe configurar el esquema de rendimiento como fuente de consultas, ya que el agente de Query Analytics no está instalado en Amazon RDS y no puede leer el registro de consultas lento. En su lugar, las consulta directamente performance_schema desde las instancias de base de datos MySQL y MariaDB para obtener métricas. Una de las características más destacadas de PMM es su [capacidad de alertar](#) y asesorar DBAs sobre los problemas que la herramienta identifica en sus bases de datos. PMM ofrece conjuntos de comprobaciones 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 monitoreo disponibles en el mercado que se pueden integrar con Amazon RDS. [Algunos ejemplos incluyen el monitoreo de bases de datos de Datadog, el monitoreo de Amazon RDS de Dynatrace y el monitoreo de bases de datos. AppDynamics](#)

Supervisión de instancias de base de datos

Una [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 de subprocesos o conexiones, 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, consistencia, aislamiento y durabilidad (ACID). InnoDB presenta [estructuras en memoria](#) (grupo de búferes, búfer de cambios, índice hash adaptativo, búfer de registro), así como [estructuras en disco](#) (espacios de tabla, tablas, índices, undo log, redo log, archivos de búfer de doble escritura). Para garantizar que su base de datos se adhiera estrictamente al modelo ACID, [el motor de almacenamiento InnoDB implementa numerosas](#) capacidades para proteger sus datos, incluidas las transacciones, la confirmación, la reversión, la recuperación de fallos, 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 ayudar a mantener la disponibilidad, integridad y seguridad de sus datos con el nivel de rendimiento esperado y satisfactorio. En función de la carga de trabajo, cada componente y función 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 para 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 monitorear estos componentes internos, compararlos con los valores de referencia definidos y generar alertas si los valores monitoreados se desvían de los valores esperados.

Como se describió anteriormente, puede usar diferentes [herramientas](#) para monitorear sus 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.

Independientemente de la herramienta de supervisión que prefiera, le recomendamos que [active el esquema de rendimiento en](#) sus instancias de base de datos MySQL y MariaDB. El [esquema](#)

[de rendimiento](#) es una función 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 función mediante el `performance_schema` parámetro. Si bien este parámetro es opcional, debe usarlo para recopilar métricas de alta resolución (un segundo) por SQL, métricas de sesión activa, eventos de espera y otra información de monitoreo detallada de bajo nivel, que recopila Amazon RDS Performance Insights.

Secciones

- [Métricas de Performance Insights para instancias de bases de datos](#)
- [CloudWatch métricas para instancias de base de datos](#)
- [Publicar métricas de Performance Insights en CloudWatch](#)

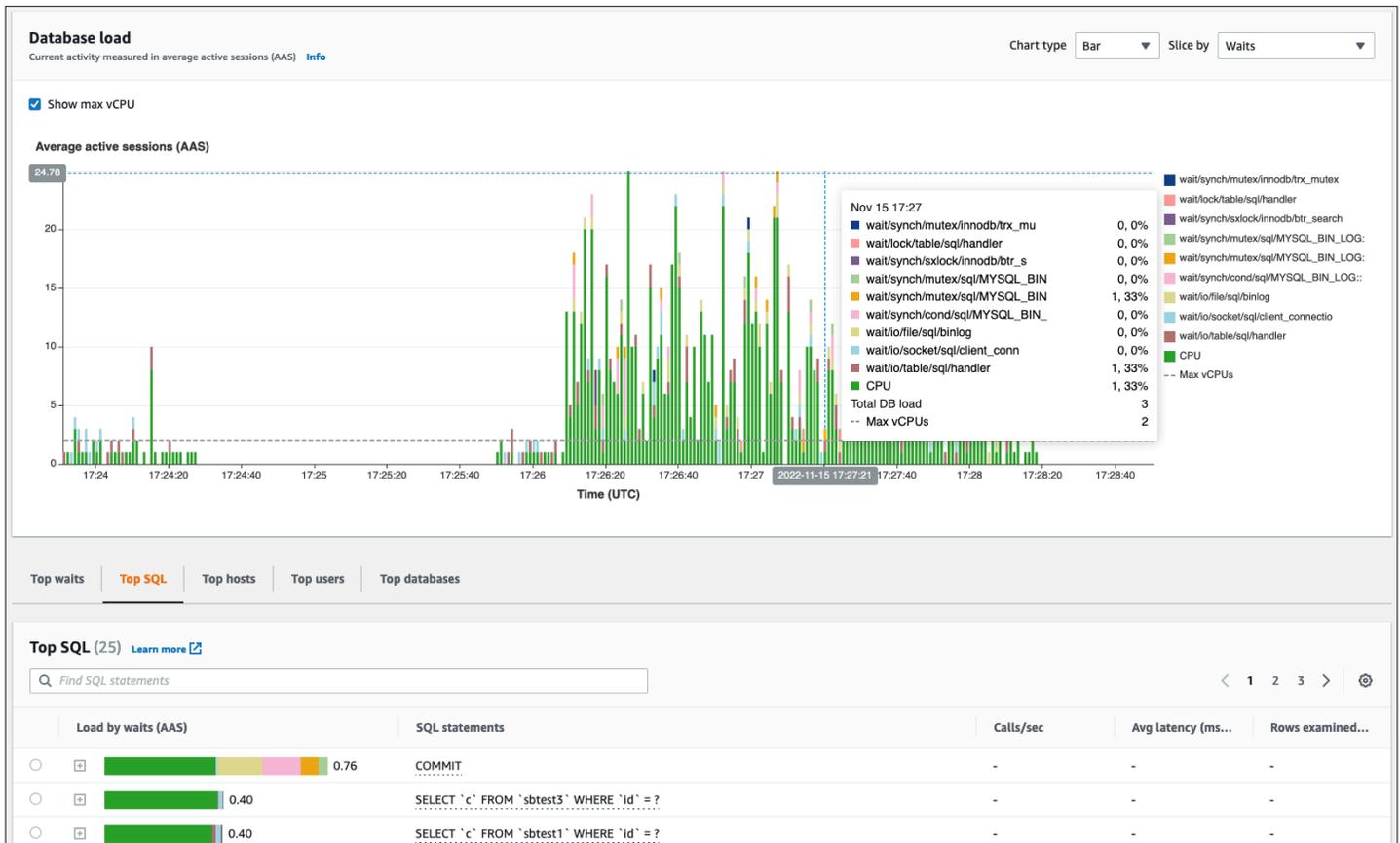
Métricas de Performance Insights para instancias de bases de datos

Performance Insights monitorea diferentes tipos de métricas, como se explica en las siguientes secciones.

Carga de base de datos

La carga de la base de datos (DBLoad) es una métrica clave de Performance Insights 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 DBLoad métrica es diferente 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 ilustración de pantalla muestra la herramienta Performance Insights.



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 operaciones de E/S físicas en el archivo de datos. Los eventos de espera son una dimensión importante para la supervisión de las bases de datos, ya que indican posibles cuellos de botella en el rendimiento. Los eventos de espera indican los recursos y las operaciones que las sentencias SQL que se ejecutan en las sesiones tardan más tiempo en esperar. Por ejemplo, el `wait/synch/mutex/innodb/trx_sys_mutex` evento se produce cuando hay una alta actividad en la base de datos con un gran número de transacciones y se produce cuando un hilo ha adquirido un bloqueo en el conjunto de búferes de InnoDB para acceder a una página en la memoria. `wait/synch/mutex/innodb/buf_pool_mutex` Para obtener información sobre todos los eventos de espera de MySQL y MariaDB, [consulte las tablas resumidas de eventos de espera](#) en la documentación de MySQL. Para entender cómo interpretar los nombres de los instrumentos,

consulte [Convenciones de nomenclatura de instrumentos del esquema de rendimiento](#) en la documentación de MySQL.

- SQL muestra qué sentencias SQL contribuyen más a la carga total de la base de datos. La tabla de dimensiones principales, que se encuentra debajo del gráfico de carga de la base de datos en Amazon RDS Performance Insights, es interactiva. Puede obtener una lista detallada de los eventos de espera asociados a la sentencia SQL haciendo clic en la barra de la columna Load by waits (AAS). Al seleccionar una sentencia SQL de la lista, Performance Insights muestra los eventos de espera asociados en el diagrama de carga de la base de datos y el texto de la sentencia SQL en la sección de texto SQL. Las estadísticas de SQL se muestran en el lado derecho de la tabla de dimensiones principales.
- Los hosts muestran los nombres de host de los clientes conectados. Esta dimensión le ayuda a identificar qué hosts clientes envían la mayor parte de la carga a la base de datos.
- Los usuarios agrupan la carga de la base de datos por los usuarios que han iniciado sesión en la base de datos.
- Las bases de datos agrupan la carga de base de datos por 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 la instancia de base de datos se reinicia. El valor de una contramétrica no se puede reducir a su valor anterior. Estas métricas representan un contador único que aumenta monótonamente.

- 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 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.

Para ver las definiciones de todas las métricas nativas, consulte [Variables de estado del servidor](#) en la documentación de MySQL.

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

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

- `I0.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 reregistro de escritura. Se calcula de la siguiente manera:

```
db.I0.Innodb_data_writes - db.I0.Innodb_log_writes - db.I0.Innodb_dblwr_writes
```

Puede visualizar las métricas de la instancia de base de datos directamente en el panel de Performance Insights. 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 siguiente ilustración.

Select metrics shown on the graph ✕

Find metrics

OS metrics (0) **Database metrics (6)** Clear all selections

▼ SQL

<input type="checkbox"/> Com_analyze	<input type="checkbox"/> Com_optimize
<input type="checkbox"/> Com_select	<input type="checkbox"/> Innodb_rows_inserted
<input type="checkbox"/> Innodb_rows_deleted	<input type="checkbox"/> Innodb_rows_updated
<input type="checkbox"/> Innodb_rows_read	<input type="checkbox"/> Questions
<input checked="" type="checkbox"/> Queries	<input type="checkbox"/> Select_full_join
<input type="checkbox"/> Select_full_range_join	<input type="checkbox"/> Select_range
<input type="checkbox"/> Select_range_check	<input checked="" type="checkbox"/> Select_scan
<input type="checkbox"/> Slow_queries	<input type="checkbox"/> Sort_merge_passes
<input type="checkbox"/> Sort_range	<input type="checkbox"/> Sort_rows
<input checked="" type="checkbox"/> Sort_scan	<input type="checkbox"/> innodb_rows_changed

▼ Locks

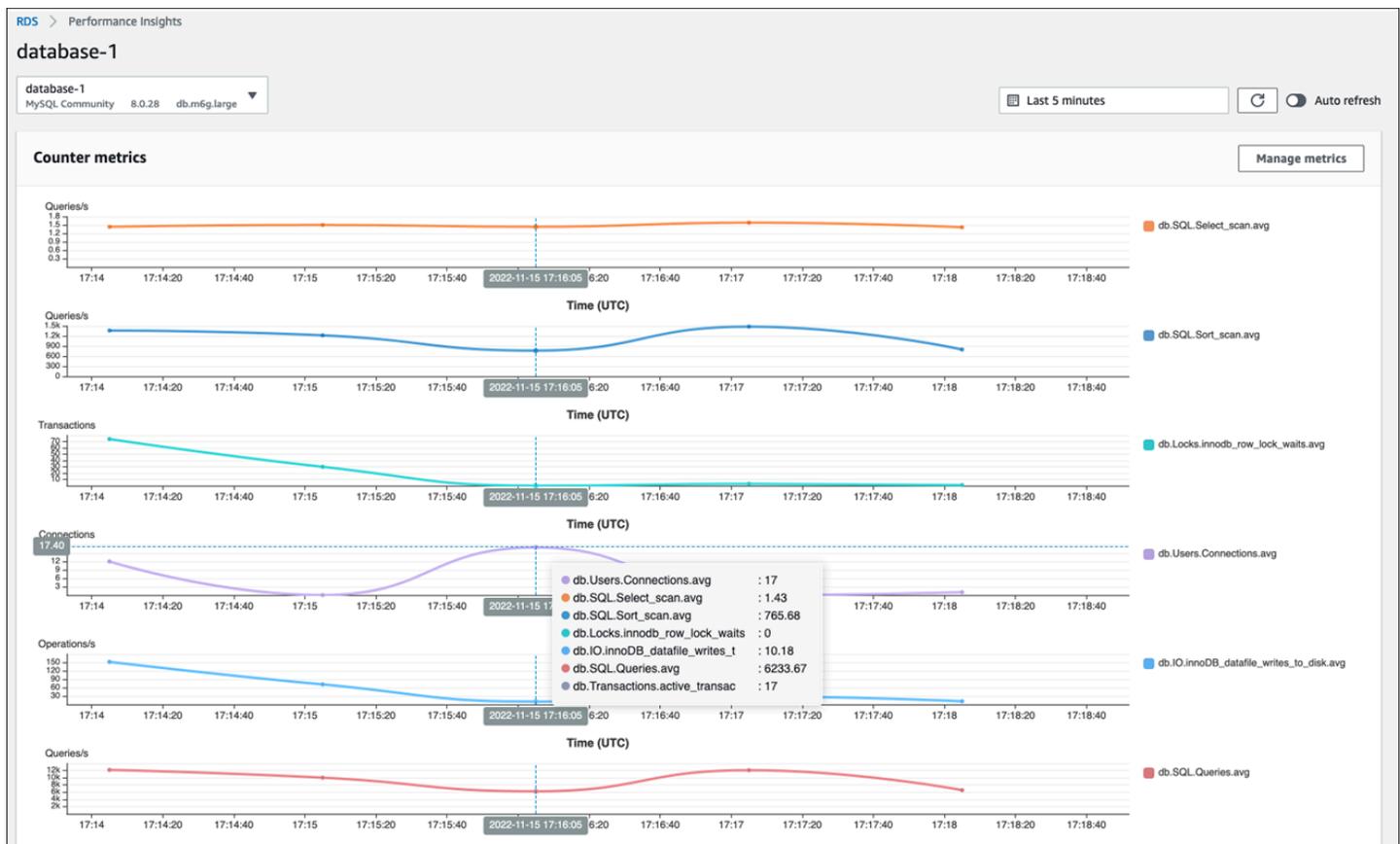
<input type="checkbox"/> Innodb_row_lock_time	<input checked="" type="checkbox"/> innodb_row_lock_waits
<input type="checkbox"/> innodb_deadlocks	<input type="checkbox"/> innodb_lock_timeouts
<input type="checkbox"/> Table_locks_immediate	<input type="checkbox"/> Table_locks_waited

▼ Users

<input checked="" type="checkbox"/> Connections	<input type="checkbox"/> Aborted_clients
<input type="checkbox"/> Aborted_connects	<input type="checkbox"/> Threads_running
<input type="checkbox"/> Threads_created	<input type="checkbox"/> Threads_connected

Cancel Update graph

Pulse el botón Actualizar gráfico para mostrar las métricas que ha seleccionado, como se muestra en la siguiente ilustración.



Estadísticas de SQL

Performance Insights recopila métricas relacionadas con el rendimiento sobre las consultas SQL para cada segundo que se ejecuta una consulta y para cada llamada SQL. En general, Performance Insights recopila [estadísticas de SQL](#) a nivel de enunciado y resumen. Sin embargo, para las instancias de base de datos MariaDB y MySQL, las estadísticas se recopilan solo a nivel de resumen.

- Las estadísticas resumidas 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 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 sentencia SQL resumida. Por ejemplo, `sql_tokenized.stats.count_star_per_sec` representa las llamadas por segundo (es decir, el número de veces por segundo que se ha ejecutado la sentencia SQL).

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

Las estadísticas de SQL están disponibles en el panel de control de Performance Insights, en la pestaña SQL principal de la tabla de dimensiones principales.

Load by waits (AAS)	SQL statements	Calls/sec	Avg laten...	Rows exa...
< 0.01	INSERT INTO `sbtest3` (`k`, `c`, `pad`) VALUES (...)/^, ...*/	3.50	0.10	0.00
< 0.01	INSERT INTO `sbtest1` (`k`, `c`, `pad`) VALUES (...)/^, ...*/	3.15	1.30	0.00
< 0.01	INSERT INTO `sbtest5` (`k`, `c`, `pad`) VALUES (...)/^, ...*/	5.53	1.00	0.00

CloudWatch métricas para instancias de bases de datos

Amazon CloudWatch también contiene métricas que Amazon RDS publica automáticamente.

Las métricas que residen en el AWS/RDS espacio de nombres son métricas a nivel de instancia, 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. Algunos ejemplos son: `CPUUtilizationWriteIOPS`, `SwapUsage`, y otros. Sin embargo, hay algunas métricas de instancias de base de datos que son aplicables a MariaDB y MySQL:

- `BinLogDiskUsage`— La cantidad de espacio en disco que ocupan los registros binarios.
- `DatabaseConnections`— El número de conexiones de red del cliente a la instancia de base de datos.
- `ReplicaLag`— El tiempo que una instancia de base de datos de réplica de lectura se retrasa 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 raíz. Sin embargo, no es posible crear alarmas en Performance Insights para 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 de sistemas operativos y bases de datos, como `os.memory.free`, `odb.Locks.InnoDB_row_lock_time`. La recopilación de métricas del sistema operativo depende de la configuración de supervisión mejorada. Si la supervisión mejorada está desactivada, las métricas del sistema operativo se recopilan una vez cada minuto. Si la supervisión mejorada está activada, se recopilan las métricas del sistema operativo durante el período de tiempo seleccionado. Para obtener más información, consulte [Activación y desactivación de la supervisión mejorada](#) en la documentación 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. La exportación del panel de métricas de Performance Insights al CloudWatch panel le proporciona una visión unificada y holística del estado de su sistema, ya que proporciona una visión general de las métricas asociadas a varios recursos del sistema, como las EC2 instancias, los recursos de Amazon Elastic File System (Amazon EFS) y los recursos de Elastic Load Balancing (ELB), junto con las métricas de la instancia 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 su instancia de base de datos alcance un umbral específico, siga las instrucciones de esa página, utilice la siguiente expresión `DB_PERF_INSIGHTS` matemática y, a continuación, elija Aplicar:

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

donde `db-BQ2TPYY7HG2GDFC7APMB3BVB3M` está el ID de recurso de su instancia de base de datos. Especifique el período (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, añada 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 de la utilización 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 de 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 forma dinámica. Cuando no hay suficiente memoria en la RAM para realizar 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 está basado en la NVMe tecnología SSD, 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 memoria adicional. Si la asignación de memoria es tan alta que agota los espacios de RAM y 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 siguientes:

Los sistemas de administración de bases de datos MySQL y MariaDB utilizan el subsistema de almacenamiento, que consta de discos que [almacenan estructuras en el disco](#), como tablas, índices,

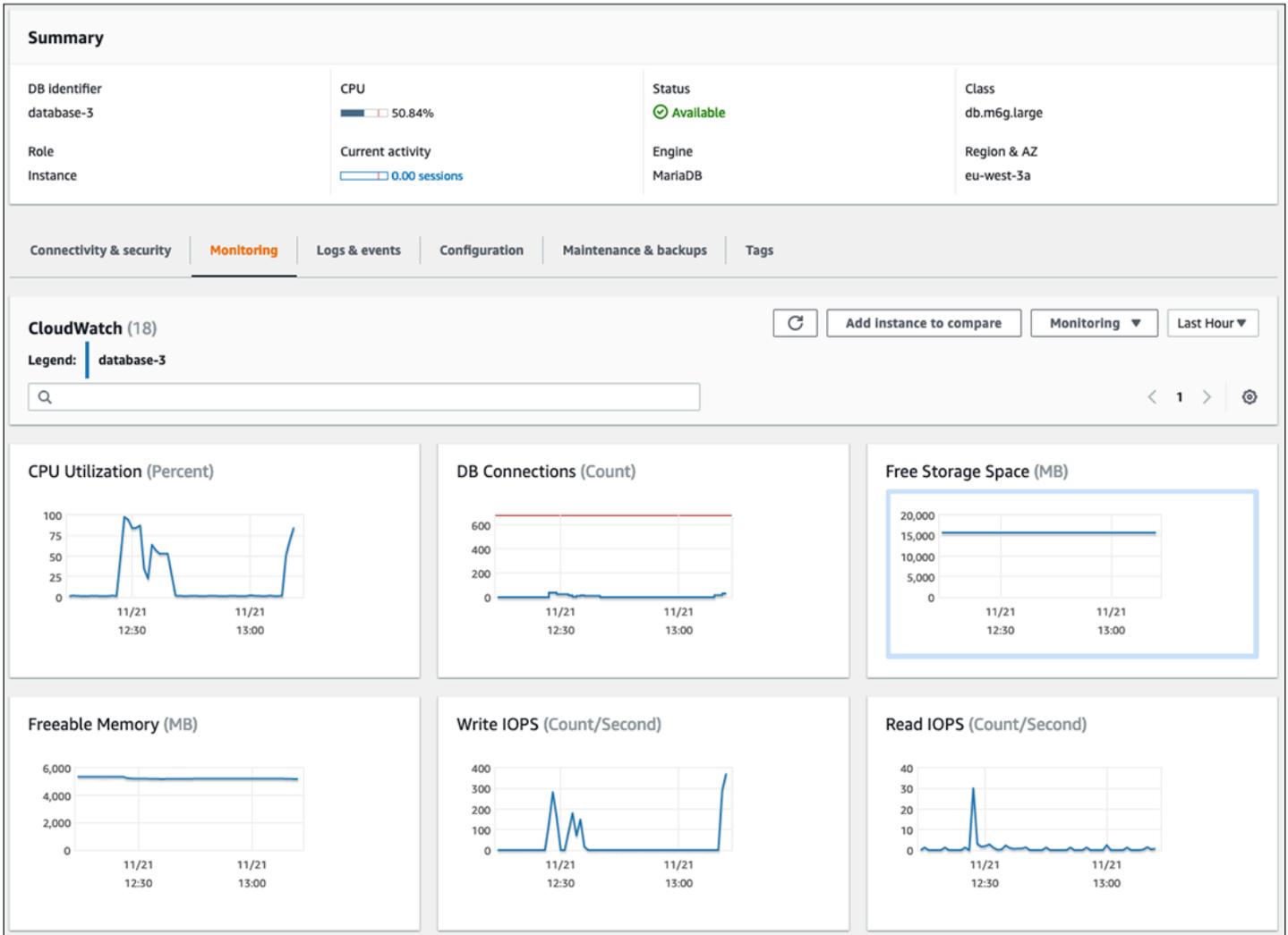
registros binarios, registros de rehacer, deshacer registros y archivos de búfer de doble escritura. Por lo tanto, la base de datos, a diferencia de otros tipos de software, debe realizar una gran actividad en el disco. Para un funcionamiento óptimo de la base de datos, es importante que supervise y 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 admitidos por el disco. Por ejemplo, las ráfagas de acceso aleatorio provocadas 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 alertas sobre la asignación de espacio en disco, ya que este tipo de errores OS `error code 28: No space left on device` pueden provocar la falta de disponibilidad y dañar la base de datos.

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 automáticamente un conjunto de métricas del sistema operativo en CloudWatch. Estas métricas están disponibles para su visualización y análisis en la consola y los CloudWatch paneles de Amazon RDS, y puede configurar alarmas en las métricas seleccionadas en CloudWatch. Entre los ejemplos se incluyen:

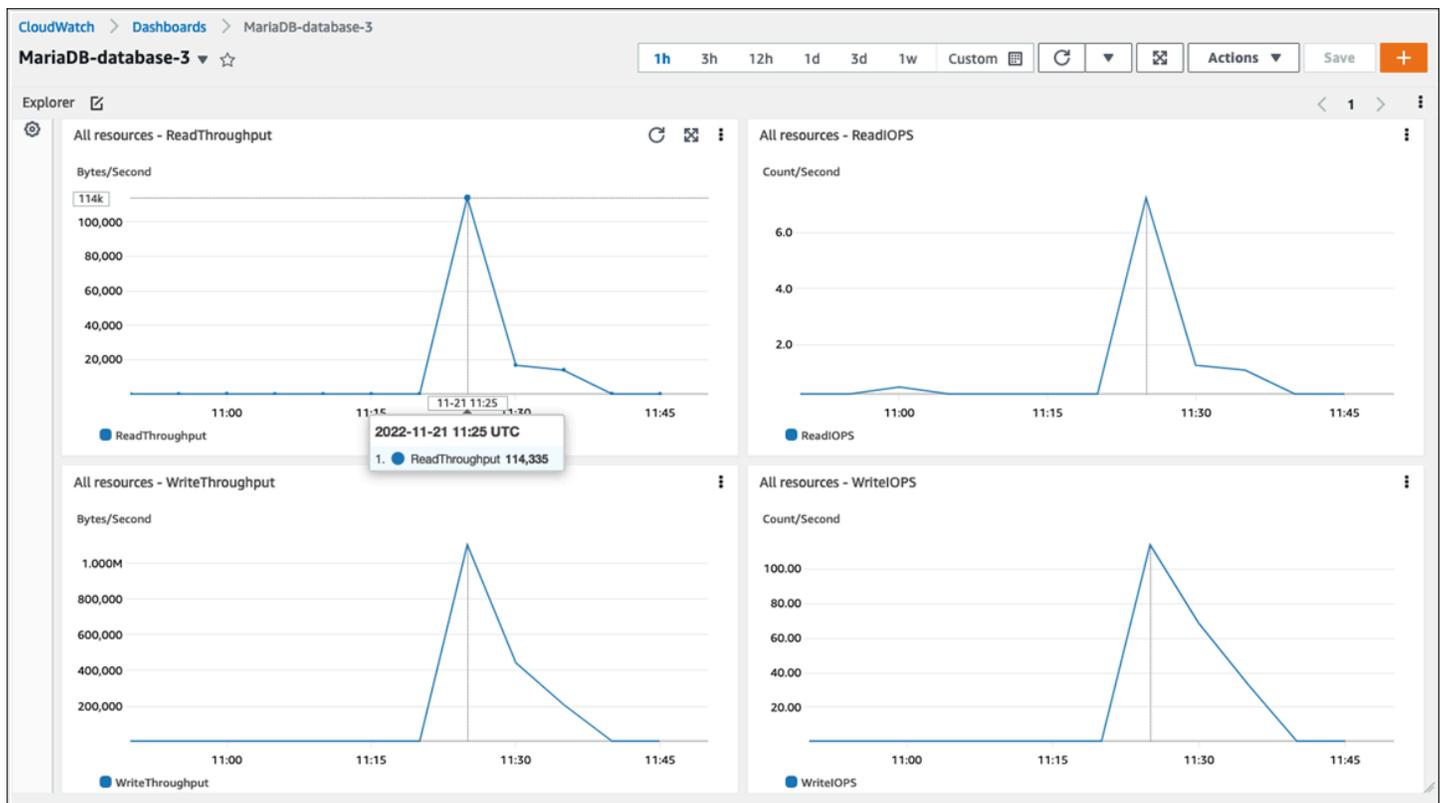
- `CPUUtilization`— El porcentaje de uso de la CPU.
- `BinLogDiskUsage`— La cantidad de espacio en disco que ocupan los registros binarios.
- `FreeableMemory`— La cantidad de memoria de acceso aleatorio disponible. Representa el valor del `MemAvailable` campo de `/proc/meminfo`.
- `ReadIOPS`— El número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

Para obtener una referencia completa de todas las métricas publicadas por Amazon RDS CloudWatch, consulte Amazon [CloudWatch Metrics for Amazon RDS](#) en la documentación de Amazon RDS.

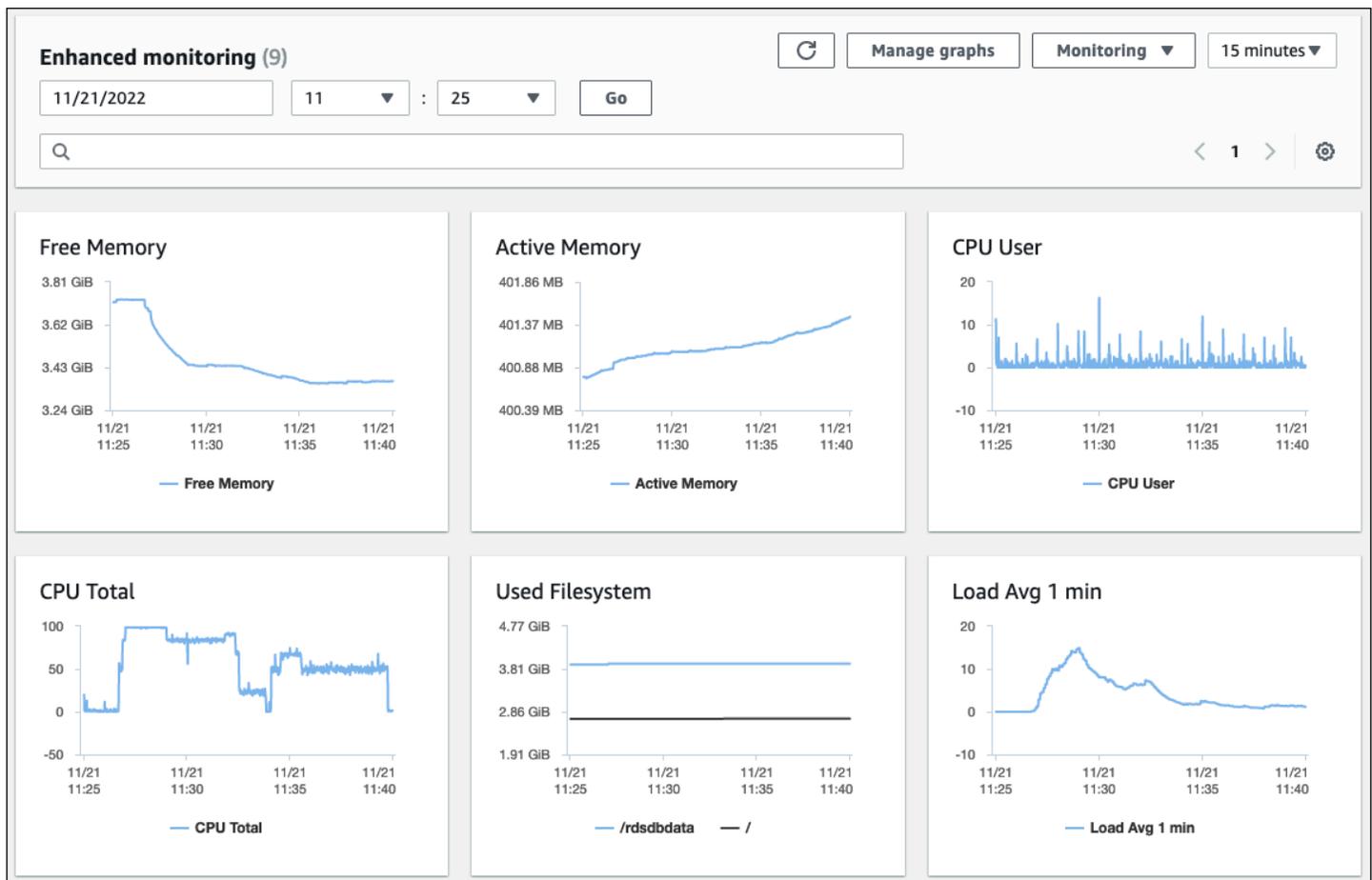
En el siguiente gráfico se muestran ejemplos de CloudWatch métricas de Amazon RDS que se muestran en la consola de Amazon RDS.



El siguiente gráfico muestra métricas similares que se muestran en el CloudWatch panel de control.



El otro conjunto de métricas del sistema operativo lo recopila [Enhanced Monitoring](#) for Amazon RDS. Esta herramienta le ofrece una mayor visibilidad del estado de sus instancias de base de datos Amazon RDS for MariaDB y Amazon RDS for MySQL, ya que proporciona métricas del sistema e información sobre los procesos del sistema operativo en tiempo real. Cuando [habilita la supervisión mejorada](#) en su 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`— El porcentaje total de la CPU en uso.
- `cpuUtilization.user`— El porcentaje de CPU utilizado por los programas de usuario.
- `memory.active`— La cantidad de memoria asignada, en kilobytes.
- `memory.cached`— La cantidad de memoria utilizada para almacenar en caché las E/S basadas en el sistema de archivos.
- `loadAverageMinute.one`— El número de procesos que solicitaron tiempo de CPU durante el último minuto.

Para obtener una lista completa de las métricas, consulte las [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 AWS procesos 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 `mysqld` proceso y sus subprocesos. Los `mysqld` subprocesos aparecen anidados debajo del proceso principal. `mysqld`

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

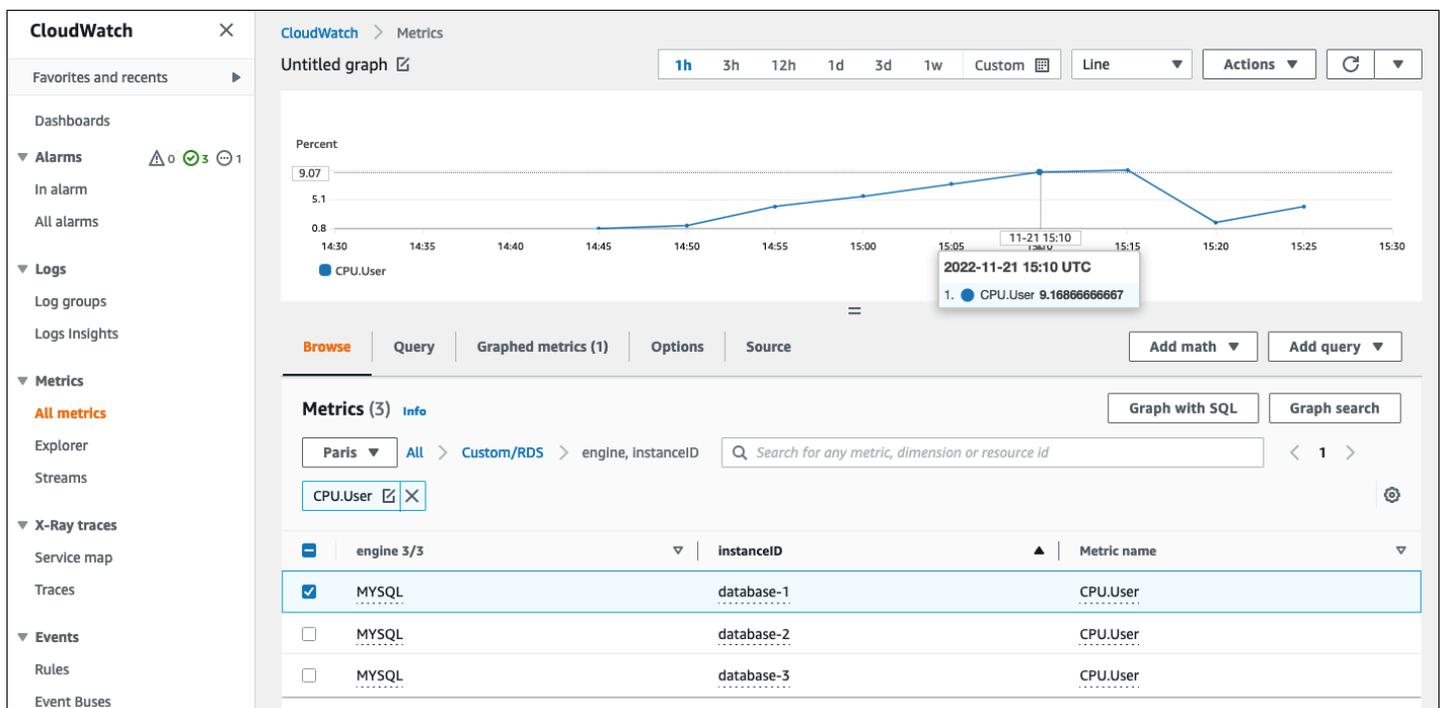
NAME	VIRT	RES	CPU%	MEM%	VMLIMIT
OS processes	1.41 GiB	106.72 MB	0.1	1.36	
RDS processes	6.18 GiB	458.25 MB	7.6	5.84	
mysqld [723]!	7.59 GiB	1.8 GiB	0	23.51	unlimited
mysqld [733]!			0		
mysqld [734]!			0		
mysqld [735]!			0		
mysqld [736]!			0		
mysqld [737]!			0		
mysqld [738]!			0		
mysqld [739]!			0		

Amazon RDS entrega las métricas de Enhanced Monitoring a su cuenta de CloudWatch Logs. Los datos de supervisión que se muestran en la consola de Amazon RDS se recuperan de CloudWatch los registros. También puede [recuperar las métricas de una instancia de base de datos como un](#)

[flujo de registro](#) desde CloudWatch Logs. Estas métricas se almacenan en formato JSON. Puede consumir la salida JSON de supervisión mejorada de CloudWatch los registros en el sistema de supervisión que prefiera.

Para mostrar gráficos en el CloudWatch panel y crear alarmas que inicien una acción si una métrica supera el umbral definido, debe crear filtros de métricas a CloudWatch partir de los CloudWatch registros. Para obtener instrucciones detalladas, consulte el [artículo de AWS Re:post](#) sobre cómo filtrar los CloudWatch registros de monitoreo mejorados para generar 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 filtrando la métrica de supervisión `cpuUtilization.user` mejorada de los registros. CloudWatch



Cuando la métrica esté disponible en el CloudWatch repositorio, podrá mostrarla y analizarla en CloudWatch paneles, aplicar más operaciones matemáticas y de consulta, y configurar una alarma para monitorear esta métrica específica y generar alertas si los valores observados no están en línea con las condiciones de alarma definidas.

Eventos, registros y pistas 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 referencia y generar alertas cuando los valores superen los umbrales definidos son prácticas recomendadas necesarias para ayudarle a lograr y mantener la fiabilidad, la disponibilidad, el rendimiento y la seguridad de sus instancias de base de datos de Amazon RDS. Sin embargo, una solución completa también debe monitorear los eventos de las bases de datos, los archivos de registro y las pistas de auditoría de las bases de datos MySQL y MariaDB.

Secciones

- [Eventos de Amazon RDS](#)
- [registros de bases de datos](#)
- [Registros de auditoría](#)

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 base 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 prácticamente EventBridge en tiempo real. Puede acceder a los eventos a través de la consola de Amazon RDS, el AWS CLI comando [describe-events](#) o la operación de la API de Amazon RDS. [DescribeEvents](#) 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

< 1 > ⚙

	Name	▲	State	▼	More options
<input type="radio"/>	ApplicationInsights/RDS-DBS/AWS/RDS/CPUUtilization/database-1/		OK		view
<input type="radio"/>	ApplicationInsights/RDS-DBS/AWS/RDS/ReadLatency/database-1/		OK		view
<input type="radio"/>	ApplicationInsights/RDS-DBS/AWS/RDS/WriteLatency/database-1/		OK		view

Recent events (9)

↻

< 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

< 1 2 3 > ⚙

	Name	▲	Last written	▼	Logs
<input type="radio"/>	error/mysql-error-running.log		November 28, 2022, 17:00 (UTC+01:00)		0 bytes
<input type="radio"/>	error/mysql-error-running.log.2022-11-28.16		November 28, 2022, 16:40 (UTC+01:00)		3.3 kB
<input type="radio"/>	error/mysql-error.log		November 29, 2022, 11:20 (UTC+01:00)		0 bytes
<input type="radio"/>	mysqlUpgrade		October 10, 2022, 17:05 (UTC+02:00)		1 kB

Amazon RDS emite diferentes tipos de eventos, incluidos eventos de instancias de base de datos, eventos de grupos de parámetros de base de datos, eventos de grupos de seguridad de base de datos, eventos de instantáneas de base de datos, eventos de proxy de RDS y eventos de despliegue azul/verde. La información incluye:

- Nombre y tipo de fuente; 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 las [categorías de eventos y los mensajes de eventos de Amazon RDS](#) en la documentación de Amazon RDS.

Le recomendamos que supervise los eventos de Amazon RDS, ya que estos eventos 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 respaldo y recuperación, acciones de conmutación por error, eventos de error, modificaciones en los grupos de seguridad y muchas otras notificaciones. Por ejemplo, si ha configurado una instancia de base de datos de réplica de lectura para mejorar el rendimiento y la durabilidad de su 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 que eventos como los que RDS-EVENT-0057 Replication on the read replica was terminated indican que su réplica de lectura ya no se sincroniza con la instancia de base de datos principal. Una notificación al equipo responsable de que se ha producido un evento de este tipo podría ayudar a mitigar el problema a tiempo. Amazon EventBridge y otros Servicios de AWS AWS Lambda, como Amazon Simple Queue Service (Amazon SQS) y Amazon Simple Notification Service (Amazon SNS), pueden ayudarlo 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 los eventos de las últimas 24 horas. Si utiliza la API de Amazon RDS AWS CLI o la API de Amazon RDS para ver los eventos, puede recuperar los eventos de los últimos 14 días mediante el comando describe-events de la siguiente manera.

```
$ 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 período de caducidad especificado o de forma permanente, puede usar [CloudWatch Logs](#) para registrar la información sobre los eventos generados por Amazon RDS. Para implementar esta solución, puede usar un tema de Amazon SNS para recibir notificaciones de eventos de Amazon RDS y, a continuación, llamar a una función de Lambda para registrar el evento en Logs. CloudWatch

1. Cree una función Lambda a la que se invocará en el evento y registre la información del evento en Logs. CloudWatch CloudWatch Logs está integrado con Lambda y proporciona una forma cómoda de registrar la información de eventos, mediante la función de impresión para. `stdout`
2. Cree un tema de SNS con una suscripción a una función de Lambda (establezca Protocol en Lambda) y configure el punto de conexión con el nombre de recurso de Amazon (ARN) de la función de Lambda que creó en el paso anterior.
3. Configure su tema de SNS para recibir notificaciones de eventos de Amazon RDS. Para obtener instrucciones detalladas, consulte el [artículo de AWS Re:post](#) sobre cómo hacer que su tema de Amazon SNS reciba notificaciones de Amazon RDS.

4. En la consola de Amazon RDS, cree una nueva suscripción a eventos. Establezca Target en el ARN y, a continuación, seleccione el tema de SNS que creó anteriormente. Defina el tipo de fuente y las categorías de eventos para incluirlas de acuerdo con sus requisitos. Para obtener 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 MySQL y MariaDB generan registros a los que puede acceder para realizar auditorías y solucionar problemas. Estos registros son:

- **Auditoría:** la pista 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 cierre del servidor (mysqld) y los mensajes de diagnóstico, como errores, advertencias y notas, que se producen durante el inicio y el apagado del servidor y mientras el servidor está en funcionamiento.
- **General:** este registro registra la actividad de cada clientemysqld, incluida 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 ha producido un error y se quiere saber exactamente a qué se ha enviado el clientemysqld.
- **Consulta lenta:** este registro proporciona un registro de las consultas SQL que tardaron mucho tiempo en realizarse.

Como práctica recomendada, debe [publicar los registros de bases de datos de Amazon RDS en Amazon CloudWatch Logs](#). Con CloudWatch Logs, puede realizar un análisis en tiempo real de los datos de registro, almacenar los datos en un almacenamiento de alta durabilidad y gestionar los datos con el agente CloudWatch Logs. Puede [acceder a los registros de su base de datos y verlos](#) desde la consola de Amazon RDS. También puede utilizar CloudWatch Logs Insights para buscar y analizar de forma interactiva los datos de registro en CloudWatch Logs. El siguiente ejemplo ilustra una consulta en el registro de auditoría que comprueba cuántas veces aparecen CONNECT los eventos en el registro, quién se conectó y desde qué cliente (dirección IP) se conectaron. El extracto del registro de auditoría podría tener este aspecto:

```
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
```

El ejemplo de consulta de Log Insights muestra que se `rdsadmin` conectaron a la base de datos `localhost` cada 5 minutos, un total de 22 veces, como se muestra en la siguiente ilustración. Estos resultados indican que la actividad se originó a partir de procesos internos de Amazon RDS, como el propio sistema de monitoreo.

CloudWatch > **Logs Insights**

Logs Insights

Select log groups, and then run a query or [choose a sample query](#).

5m 30m **1h** 3h 12h Custom

Select log group(s)

/aws/rds/instance/database-1/audit

```

1 fields @timestamp, @message
2 | filter @message like /(?!)(CONNECT)/
3 | parse @message '*,*,*' as @instance,@user
4 | parse @message /(?<@ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/
5 | stats count() AS counter by @user, @ip
6 | sort by @user desc, @counter desc
7 | limit 50
    
```

Run query Cancel Save History

Queries are allowed to run for up to 15 minutes.

Logs Visualization Export results Add to dashboard

Showing 1 of 22 records matched
 22 records (2.3 kB) scanned in 3.2s @ 6 records/s (746.057 B/s)

#	@user	@ip	counter
▼ 1	rdsadmin		22

Field Value

@ip

@user rdsadmin

counter 22

Los eventos de registro suelen incluir mensajes importantes que desea contar, como advertencias o errores sobre las operaciones asociadas a las instancias de base de datos 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 desee supervisar estas entradas para comprender la tendencia de sus errores.

Puede [crear CloudWatch métricas personalizadas a partir de los registros de Amazon RDS mediante filtros](#) que permiten la supervisión automática de los registros de la base de datos de Amazon RDS, monitorizar 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](#), por ejemplo, `ERROR`. Establezca el patrón de filtro en `ERROR` y el valor métrico en `1`. El filtro detectará todos los registros de registro que contengan la palabra clave `ERROR` e incrementará el recuento en `1` por cada evento de registro que contenga la palabra «`ERROR`». Después de crear el filtro, puede configurar una alarma para que le notifique en caso de que se detecten errores en el registro de errores de MySQL o MariaDB.

Para obtener más información sobre la supervisión del registro de consultas lento y el registro de errores mediante la creación de un CloudWatch panel y el uso de CloudWatch Logs Insights, consulte la entrada del blog [Creating an Amazon CloudWatch Dashboard to Monitoring Amazon RDS y Amazon Aurora MySQL](#).

Registros de seguimiento de auditoría

El registro de auditoría (o registro de auditoría) proporciona un registro cronológico y relevante para la seguridad de los eventos ocurridos en su entorno. Cuenta de AWS Incluye eventos para Amazon RDS, que proporcionan pruebas documentales de la secuencia de actividades que han afectado a su base de datos o a su entorno de nube. En Amazon RDS for MySQL o MariaDB, el uso de la pista de auditoría implica:

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

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

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

- Acciones realizadas 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 privilegiados

La pista de auditoría de la base de datos intenta responder a estas preguntas típicas: ¿Quién ha visto o modificado los datos confidenciales de su base de datos? ¿Cuándo ocurrió esto? ¿Desde dónde accedió un usuario específico a los datos? ¿Los usuarios privilegiados abusaron de sus derechos de acceso ilimitado?

Tanto MySQL como MariaDB implementan la función de registro de auditoría de la instancia de base de datos mediante el complemento de auditoría MariaDB. Este complemento registra la actividad de la base de datos, como el inicio de sesión 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 obtener más información, consulte la [compatibilidad del complemento de auditoría MariaDB para MySQL](#) en la documentación de Amazon RDS. Los registros del registro de auditoría se almacenan en un formato específico, según lo define el complemento. Puede encontrar más detalles sobre el formato del registro de auditoría en la documentación del [servidor MariaDB](#).

El Nube de AWS servicio proporciona el registro de auditoría de su AWS cuenta. [AWS CloudTrail](#) CloudTrail captura las llamadas a la API de Amazon RDS como eventos. Se registran todas las acciones de Amazon RDS. CloudTrail proporciona un registro de las acciones en Amazon RDS realizadas por un usuario, rol u otro AWS servicio. Los eventos incluyen las acciones realizadas en la consola de AWS administración AWS CLI, AWS SDKs y APIs.

Ejemplo

En un escenario de auditoría típico, es posible que necesite combinar las AWS CloudTrail rutas 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 su instancia de base de datos de Amazon RDS (por ejemplo `datatbase-1`) se hayan modificado y su tarea consista en identificar quién realizó la modificación, qué se cambió y cuándo se produjo el cambio.

Para llevar a cabo la tarea, siga estos pasos:

1. Enumere los eventos de Amazon RDS que ocurrieron 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 el AWS CLI para buscar CloudTrail eventos](#) en la región en la que `database-1` se implementa, en el período de tiempo cercano al evento de Amazon RDS descubierto en el paso 1 y dónde `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 CloudTrail evento revela que, User1 con el rol Role1 de la AWS cuenta 111122223333, se modificó el grupo de parámetros de base de datos mariadb10-6-test, que utilizaba la instancia de base de datos en. database-1 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

Funciones adicionales CloudTrail y CloudWatch de registro

Puede solucionar los incidentes operativos y de seguridad de los últimos 90 días consultando el historial de eventos en la CloudTrail consola. Para ampliar el período de retención y aprovechar las funciones 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 un máximo de siete años. Además, el servicio admite consultas SQL complejas que ofrecen una visión más profunda y personalizable de los eventos que las vistas que proporcionan las simples búsquedas de valores clave en el historial de eventos.

Para monitorear sus registros de auditoría, configurar alarmas y recibir notificaciones cuando se produzca una actividad específica, debe [configurarlos para enviar sus CloudTrail registros a Logs](#). CloudWatch Una vez que los registros de seguimiento se hayan almacenado como CloudWatch registros, puede definir filtros de métricas para evaluar los eventos del registro para que coincidan con términos, frases o valores, y asignar métricas a los filtros de métricas. Además, puede crear CloudWatch alarmas que se generen de acuerdo con los umbrales y los períodos de tiempo que especifique. Por ejemplo, puede configurar alarmas que envíen notificaciones a los equipos

responsables para que puedan tomar las medidas adecuadas. También puede configurarlo CloudWatch para que ejecute automáticamente una acción en respuesta a una alarma.

Alertas

Las alertas son una de las fuentes de información más importantes en lo que respecta a la seguridad, la disponibilidad, el rendimiento y la fiabilidad de la infraestructura y los servicios de TI. Notifican e informan a sus equipos de TI sobre las amenazas de seguridad actuales, las interrupciones, los problemas de rendimiento o los fallos del sistema.

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

Las alertas de incidentes se producen cuando las herramientas de supervisión generan alertas para notificar a tu equipo y a las herramientas automatizadas (en el caso de los elementos que se pueden procesar automáticamente) sobre cambios, acciones de alto riesgo o fallos en el entorno de TI. Las alertas de TI son la primera línea de defensa contra las interrupciones o cambios del sistema que pueden convertirse en incidentes graves. Al monitorear 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 gestión de alertas es establecer procedimientos estandarizados y eficientes para gestionar los eventos e incidentes relacionados con la 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 acciones, activar y desactivar alarmas](#)

CloudWatch alarmas

Cuando opera sus instancias de base de datos de Amazon RDS, quiere monitorizar y generar alertas sobre distintos tipos de métricas, eventos y seguimientos. En el caso de las bases de datos MySQL y [MariaDB](#), [las fuentes de información fundamentales son las métricas de las instancias](#) de base de datos, [las métricas del sistema operativo](#), [los eventos](#), [los registros](#) y las pistas de auditoría. Le recomendamos que utilice [CloudWatch 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 CPUUtilization métrica (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 la utilización de la CPU en cualquier instancia de base de datos es superior al 80 por ciento durante el período de evaluación de 5 minutos.

CloudWatch > Alarms > Create alarm

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Specify metric and conditions

Metric

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Percent

10.47

10.11

9.75

12:00 13:00 14:00

● CPUUtilization

Namespace
AWS/RDS

Metric name
CPUUtilization

Statistic
Average

Period
5 minutes

Conditions

Threshold type

Static
Use a value as a threshold

Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition.

Greater
> threshold

Greater/Equal
>= threshold

Lower/Equal
<= threshold

Lower
< threshold

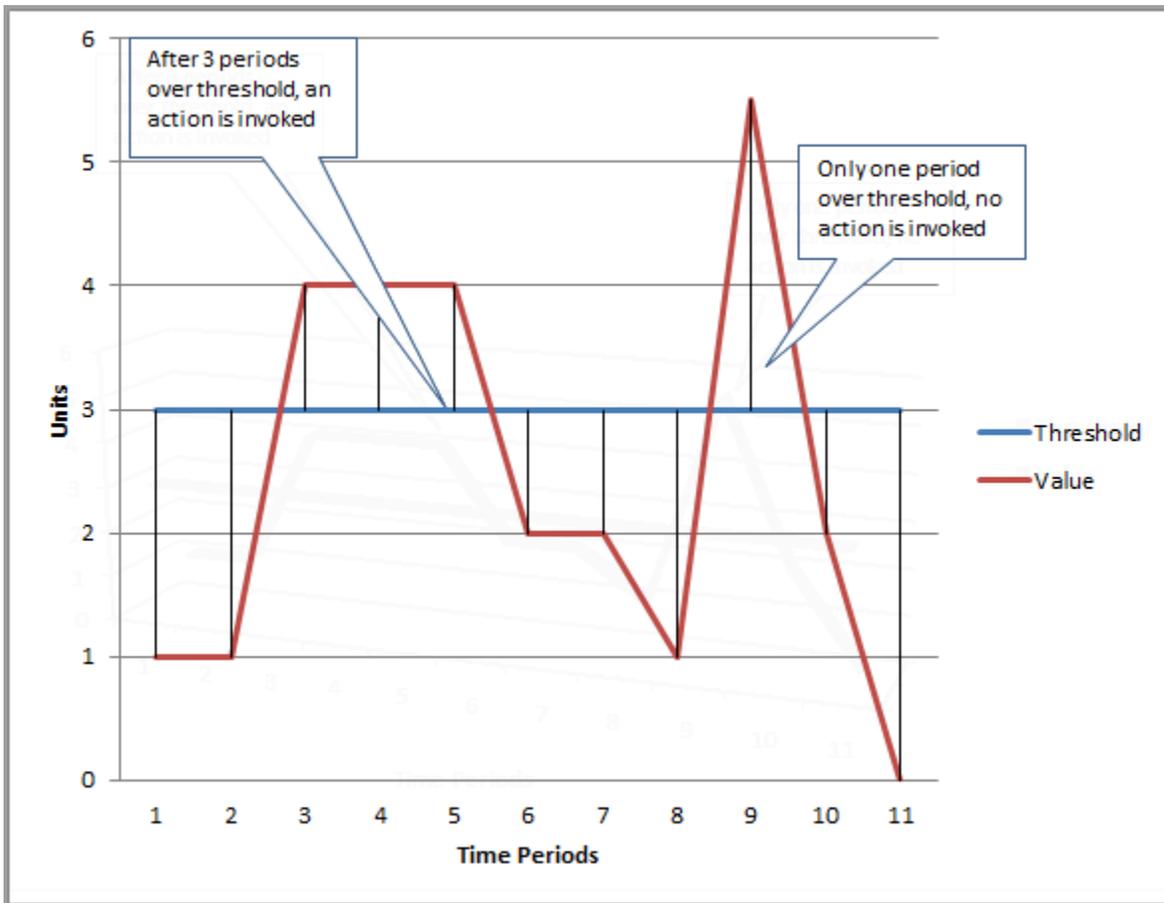
than...

Define the threshold value.

80

Must be a number

Esto significa que la alarma se activa si alguna de sus bases de datos experimenta un uso elevado de la CPU (más del 80 por ciento) durante 5 minutos o más. ALARM La alarma permanece activa si, de vez en cuando, la CPU alcanza un nivel de utilización superior al 80 por ciento durante un breve período de tiempo y, después, vuelve a caer por debajo del umbral. OK El siguiente gráfico ilustra esta lógica.



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 métrica puede enviar mensajes a Amazon SNS, que, a su vez, puede realizar una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo.
- Una alarma compuesta se basa en una expresión de regla, que evalúa los estados de varias alarmas y entra en ese ALARM estado solo si se cumplen todas las condiciones de la regla. Las alarmas compuestas se utilizan normalmente para reducir la cantidad de alertas innecesarias. Por ejemplo, es posible que tenga una alarma compuesta que contenga varias alarmas métricas que estén configuradas para no realizar ninguna acción. La alarma compuesta enviaría una alerta cuando todas las alarmas métricas individuales de la compuesta ya estén en el 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, como se ha explicado anteriormente en las secciones de [supervisión](#)

del sistema operativo y [Eventos, registros y registros de auditoría](#), puede utilizar 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.

The screenshot displays the Amazon EventBridge console interface. On the left is a navigation sidebar with categories like Developer resources, Buses, Pipes, and Integration. The main area is titled 'Amazon EventBridge > Rules'. It includes a 'Rules' section with a descriptive text: 'A rule watches for specific types of events. When a matching event occurs, the event is routed to the targets associated with the rule. A rule can be associated with one or more targets.' Below this is a 'Select event bus' section with a dropdown menu currently showing 'default'. Further down is a 'Rules (2/17)' section containing a search bar with 'rds', a '2 matches' indicator, and a table of rules. The table has columns for Name, Status, Type, and Description. Two rules are visible: 'rds-shutdown-database-3' and 'rds-startup-database-3', both with a green checkmark and the word 'Enabled' in green text, and a 'Standard' type.

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

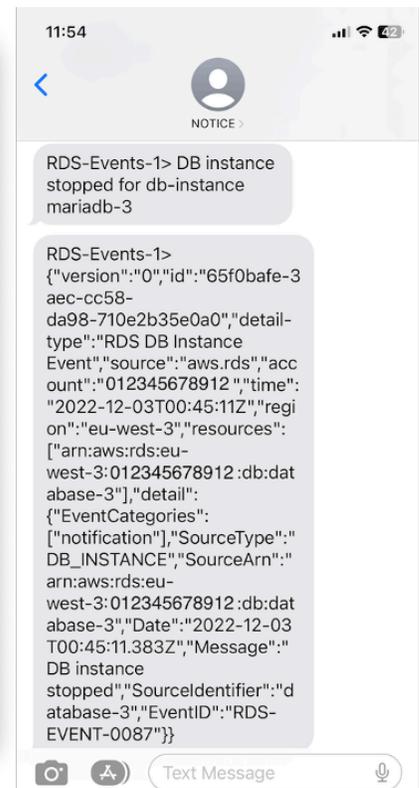
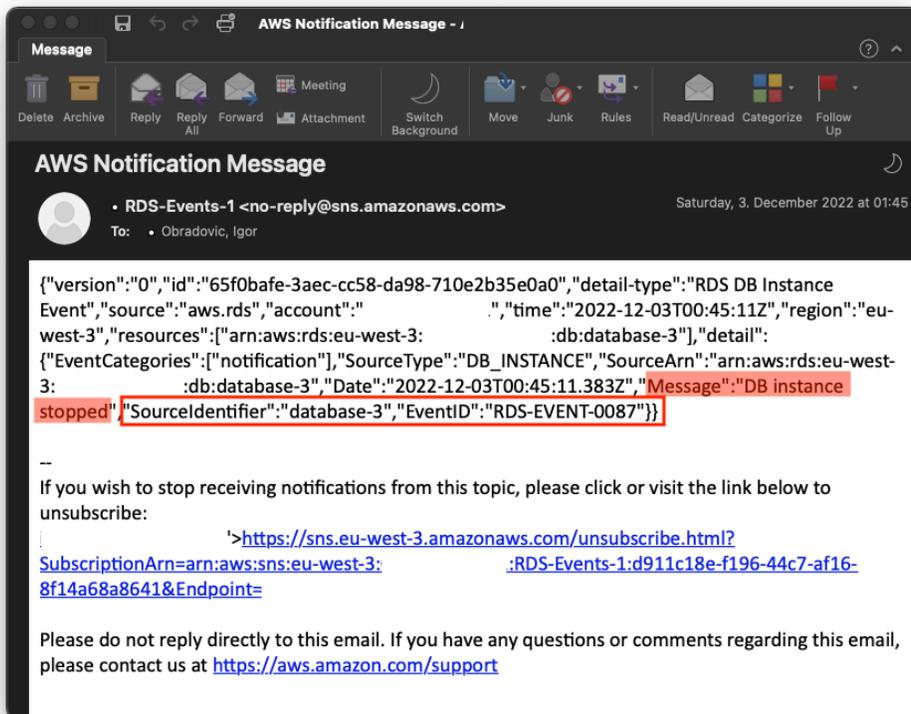
```
{
  "source": ["aws.rds"],
  "detail-type": ["RDS DB Instance Event"],
```

```

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

```

Esta regla supervisa `database-3` únicamente la instancia de base de datos y vigila el `RDS-EVENT-0087` evento. Cuando EventBridge detecta el evento, lo envía a un recurso o punto final, conocido como [destino](#). Aquí puede especificar la acción que desea realizar 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, Amazon API Gateway AWS Batch, un plan de respuesta en Incident Manager, una capacidad de y muchos otros. AWS Systems Manager 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 el objetivo 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. EventBridgea 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 siguiente ilustración) y un SMS.



Especificar acciones y habilitar y deshabilitar las alarmas

Puede usar una CloudWatch alarma para especificar qué acciones debe realizar la alarma cuando cambia entre los estados OKALARM, yINSUFFICIENT_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 EC2 (Amazon) 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 necesite gestionar las alarmas; por ejemplo, desactivar automáticamente una alarma durante los cambios de configuración planificados o las pruebas y, a continuación, volver a activar la alarma cuando finalice la acción 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 [DisableAlarmActions](#) de la API o los [enable-alarm-actions](#) comandos [disable-alarm-actions](#) y del AWS CLI. [EnableAlarmActions](#) También puede ver el historial de alarmas en la CloudWatch consola o mediante la acción de la [DescribeAlarmHistory](#) API o el [describe-alarm-history](#) comando 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 obtener más información sobre cómo migrar sus bases de datos relacionales a Nube de AWS, consulte la siguiente estrategia en el sitio web de la AWS Guía prescriptiva:

- [Estrategia de migración para bases de datos relacionales](#)

Puede explorar los patrones de migración de las bases de datos en la [Guía AWS prescriptiva](#) para step-by-step obtener instrucciones sobre las bases de datos relacionales específicas que se ejecutan en el sistema Nube de AWS, incluidas las tareas relacionadas con la supervisión, la migración y la gestión de datos.

Para obtener más ayuda, consulte los siguientes recursos:

- [Guía del usuario de Amazon Relational Database Service](#)
- [Guía CloudWatch del usuario de Amazon](#)
- [Amazon RDS FAQs](#)
- [Performance Insights FAQs](#) (Información sobre rendimiento)
- [Entregue las contramétricas de Amazon RDS Performance Insights a un proveedor de servicios de monitoreo del rendimiento de aplicaciones externo mediante Amazon CloudWatch Metrics Stream](#) (entrada AWS del blog)
- [Creación de un CloudWatch panel de Amazon para monitorear Amazon RDS y Amazon Aurora MySQL](#) (entrada AWS del blog)
- [Optimización de Amazon RDS para MySQL con Performance Insights AWS](#) (entrada del blog)

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 Performance Insights	Se actualizó la sección sobre la publicación de métricas de Performance Insights para CloudWatch incluir la información más reciente.	11 de marzo de 2025
Información actualizada sobre los exportadores	Se actualizó la información sobre los exportadores y se agregaron pautas 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: migre su base de datos Oracle local a la edición compatible con PostgreSQL de Amazon Aurora.
- **Redefinir la plataforma (transportar y redefinir):** traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Amazon Relational Database Service (Amazon RDS) para Oracle en el. Nube de AWS
- **Recomprar (readquirir):** cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- **Volver a alojar (migrar mediante lift-and-shift):** traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Oracle en una EC2 instancia del. Nube de AWS
- **Reubicar:** (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- **Retener (revisitar):** conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

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

A

ABAC

Consulte control de [acceso basado en atributos](#).

servicios abstractos

Consulte [servicios gestionados](#).

ACID

Consulte [atomicidad, consistencia, aislamiento y durabilidad](#).

migración activa-activa

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

migración activa-pasiva

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

función agregada

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

IA

Véase [inteligencia artificial](#).

AIOps

Consulte las [operaciones de inteligencia artificial](#).

anonimización

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

antipatronos

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

control de aplicaciones

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

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo 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

Un bot malo

Un [bot](#) destinado a interrumpir o causar daño a personas u organizaciones.

BCP

Consulte la [planificación de la continuidad del negocio](#).

gráfico de comportamiento

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

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también [endianness](#).

clasificación binaria

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

filtro de floración

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

implementación azul/verde

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

bot

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

botnet

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

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 con cristales rotos

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio (BCP)

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

C

CAF

[Consulte el marco AWS de adopción de la nube.](#)

despliegue canario

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

CCoE

Consulte [Cloud Center of Excellence](#).

CDC

Consulte la [captura de datos de cambios](#).

captura de datos de cambio (CDC)

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

ingeniería del caos

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

CI/CD

Consulte la [integración continua y la entrega continua](#).

clasificación

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

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

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

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCoE, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinención: 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 la [base de datos de administración de la configuración](#).

repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Los repositorios en la nube más comunes incluyen GitHub o 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 aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

desviación de configuración

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

base de datos de administración de configuración (CMDB)

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

paquete de conformidad

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

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD is commonly described as a pipeline. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte [Beneficios de la entrega continua](#). CD también puede significar implementación continua. Para obtener más información, consulte [Entrega continua frente a implementación continua](#).

CV

Vea la [visión artificial](#).

D

datos en reposo

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

clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad

del AWS Well-Architected Framework. Para obtener más información, consulte [Clasificación de datos](#).

desviación de datos

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

datos en tránsito

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

malla de datos

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

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de datos (DDL)

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

lenguaje de manipulación de datos (DML)

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

DDL

Consulte el [lenguaje de definición de bases](#) de datos.

conjunto profundo

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

aprendizaje profundo

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

defense-in-depth

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

administrador delegado

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

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

Implementación

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

entorno de desarrollo

Consulte [entorno](#).

control de detección

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

asignación de flujos de valor para el desarrollo (DVSM)

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

gemelo digital

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

tabla de dimensiones

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

desastre

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

recuperación de desastres (DR)

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

DML

Consulte el lenguaje de manipulación de [bases de datos](#).

diseño basado en el dominio

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

DR

Consulte [recuperación ante desastres](#).

detección de deriva

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

DVSM

Consulte [el mapeo del flujo de valor del desarrollo](#).

E

EDA

Consulte el [análisis exploratorio de datos](#).

EDI

Véase [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 nube, la computación](#) perimetral puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

El intercambio automatizado de documentos comerciales entre organizaciones. Para obtener más información, consulte [Qué es el intercambio electrónico de datos](#).

cifrado

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

clave de cifrado

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

endianidad

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

punto de conexión

[Consulte el punto final del servicio](#).

servicio de punto de conexión

Servicio que puede alojar en una nube privada virtual (VPC) para compartir con otros usuarios. Puede crear un servicio de punto final AWS PrivateLink y conceder permisos a otros directores

Cuentas de AWS o a AWS Identity and Access Management (IAM). Estas cuentas o entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte [Creación de un servicio de punto de conexión](#) en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

planificación de recursos empresariales (ERP)

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

cifrado de sobre

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

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 una canalización de CI/CD, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las epopeyas AWS de seguridad de CAF incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección

de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la [Guía de implementación del programa](#).

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 datos

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

fallan rápidamente

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

límite de aislamiento de fallas

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

rama de característica

Consulte la [sucursal](#).

características

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

importancia de las características

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

transformación de funciones

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

indicaciones de unos pocos pasos

Proporcionar a un [LLM](#) un pequeño número de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que realice una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, en el que los modelos aprenden a partir de ejemplos (planos) integrados en las instrucciones. Las indicaciones con pocas tomas pueden ser eficaces para tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. [Consulte también el apartado de mensajes sin intervención](#).

FGAC

Consulte el control [de acceso detallado](#).

control de acceso preciso (FGAC)

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

migración relámpago

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

FM

Consulte el [modelo básico](#).

modelo de base (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 obtener más información, consulte [Qué son los modelos básicos](#).

G

IA generativa

Un subconjunto de modelos de [IA](#) que se han entrenado con grandes cantidades de datos y que pueden utilizar un simple mensaje de texto para crear contenido y artefactos nuevos, como imágenes, vídeos, texto y audio. Para obtener más información, consulte [Qué es la IA generativa](#).

bloqueo geográfico

Consulta [las restricciones geográficas](#).

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

imagen dorada

Instantánea de un sistema o software que se utiliza 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 GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

HA

Consulte la [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 retenidos

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de aprendizaje [automático](#). Puede utilizar los datos de reserva para evaluar el rendimiento del modelo comparando 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, las revisiones suelen realizarse fuera del flujo de trabajo habitual de las versiones.

DevOps

periodo de hiperatención

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

I

IaC

Vea [la infraestructura como código](#).

políticas basadas en identidad

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

aplicación inactiva

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

IIoT

Consulte [Internet de las cosas industrial](#).

infraestructura inmutable

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

VPC entrante (de entrada)

En una arquitectura de AWS cuentas múltiples, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La [arquitectura 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.

I

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial (IIoT)

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

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 IIoT?](#).

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 la [biblioteca de información de TI](#).

ITSM

Consulte [Administración de servicios de TI](#).

L

control de acceso basado en etiquetas (LBAC)

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

zona de aterrizaje

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

modelo de lenguaje grande (LLM)

Un modelo de [IA](#) de aprendizaje profundo que se entrena previamente con una gran cantidad de datos. Un LLM puede realizar múltiples 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

Ver [7 Rs](#).

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Véase también [endianness](#).

LLM

Véase un modelo de lenguaje [amplio](#).

entornos inferiores

Véase [entorno](#).

M

machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del

Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte [Machine learning](#).

rama principal

Ver [sucursal](#).

malware

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

servicios gestionados

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

sistema de ejecución de fabricación (MES)

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

MAP

Consulte [Migration Acceleration Program](#).

mecanismo

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

cuenta de miembro

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

MES

Consulte el [sistema de ejecución de la fabricación](#).

Transporte telemétrico de Message Queue Queue (MQTT)

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

microservicio

Un servicio pequeño e independiente que se comunica a través de 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: realoje la migración a Amazon EC2 con AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Una herramienta en línea que proporciona información para validar el modelo de negocio para migrar a. Nube de AWS La MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La [herramienta MPA](#) (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

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

estrategia de migración

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

ML

[Consulte el aprendizaje automático](#).

modernización

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

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte [Descomposición de monolitos en microservicios](#).

MAPA

Consulte [la evaluación de la cartera de migración](#).

MQTT

Consulte [Message Queue Queue Telemetría](#) y Transporte.

clasificación multiclase

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

infraestructura mutable

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

O

OAC

[Consulte el control de acceso de origen.](#)

OAI

Consulte la [identidad de acceso de origen](#).

OCM

Consulte [gestión del cambio organizacional](#).

migración fuera de línea

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

OI

Consulte [integración de operaciones](#).

OLA

Véase el [acuerdo a nivel operativo](#).

migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir

funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

OPC-UA

Consulte [Open Process Communications: arquitectura unificada](#).

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

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

acuerdo de nivel operativo (OLA)

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

revisión de la preparación operativa (ORR)

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

tecnología operativa (OT)

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

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

administración del cambio organizacional (OCM)

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

control de acceso de origen (OAC)

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

identidad de acceso de origen (OAI)

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

ORR

Consulte la revisión de [la preparación operativa](#).

OT

Consulte la [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 la [información de identificación personal](#).

manual de estrategias

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

PLC

Consulte [controlador lógico programable](#).

PLM

Consulte la [gestión del ciclo de vida del producto](#).

policy

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

persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de

implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades. Para obtener más información, consulte [Habilitación de la persistencia de datos en los microservicios](#).

evaluación de cartera

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

predicate

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

pulsar un predicado

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

control preventivo

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

entidad principal

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

privacidad desde el diseño

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

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

gestión del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte [el entorno](#).

controlador lógico programable (PLC)

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

encadenamiento rápido

Utilizar la salida de una solicitud de [LLM](#) como entrada para la siguiente solicitud para generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en subtareas 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)

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

Q

plan de consulta

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

regresión del plan de consulta

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

R

Matriz RACI

Véase [responsable, responsable, consultado, informado \(RACI\)](#).

RAG

Consulte [Retrieval Augmented Generation](#).

ransomware

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

Matriz RASCI

Véase [responsable, responsable, consultado, informado \(RACI\)](#).

RCAC

Consulte control de [acceso por filas y columnas](#).

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

Ver [7 Rs](#).

objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Ver [7 Rs.](#)

Región

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

regresión

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

volver a alojar

Consulte [7 Rs.](#)

versión

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

trasladarse

Ver [7 Rs.](#)

redefinir la plataforma

Ver [7 Rs.](#)

recompra

Ver [7 Rs.](#)

resiliencia

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

política basada en recursos

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

matriz responsable, confiable, consultada e informada (RACI)

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

control receptivo

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

retain

Consulte [7 Rs](#).

jubilarse

Ver [7 Rs](#).

Generación aumentada de recuperación (RAG)

Tecnología de [inteligencia artificial generativa](#) en la que un máster [hace referencia](#) a una fuente de datos autorizada que se encuentra fuera de sus fuentes de datos de formación antes de generar una respuesta. Por ejemplo, un modelo RAG podría realizar una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para obtener más información, consulte [Qué es](#) el RAG.

rotación

Proceso de actualizar periódicamente un [secreto](#) para dificultar el acceso de un atacante a las credenciales.

control de acceso por filas y columnas (RCAC)

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

RPO

Consulte el [objetivo del punto de recuperación](#).

RTO

Consulte el [objetivo de tiempo de recuperación](#).

manual de procedimientos

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

S

SAML 2.0

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

SCADA

Consulte el [control de supervisión y la adquisición de datos](#).

SCP

Consulte la [política de control de servicios](#).

secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulta [¿Qué hay en un secreto de Secrets Manager?](#) en la documentación de Secrets Manager.

seguridad desde el diseño

Un 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 principales de controles de seguridad: [preventivos](#), [de detección](#), con [capacidad](#) de [respuesta](#) y [proactivos](#).

refuerzo de la seguridad

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

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

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

automatización de la respuesta de seguridad

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

cifrado del servidor

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

política de control de servicio (SCP)

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)

[Una métrica objetivo que representa el estado de un servicio, medido mediante un indicador de nivel de servicio.](#)

modelo de responsabilidad compartida

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

SIEM

Consulte [la información de seguridad y el sistema de gestión de eventos](#).

punto único de fallo (SPOF)

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

SLA

Consulte el acuerdo [de nivel de servicio](#).

SLI

Consulte el indicador de [nivel de servicio](#).

SLO

Consulte el objetivo de nivel de [servicio](#).

split-and-seed modelo

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

SPOF

Consulte el [punto único de falla](#).

esquema en forma de estrella

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

patrón de higo estrangulador

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

subred

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

supervisión, control y adquisición de datos (SCADA)

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

cifrado simétrico

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

pruebas sintéticas

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

indicador del sistema

Una técnica para proporcionar contexto, instrucciones o pautas a un [LLM](#) para dirigir su comportamiento. Las indicaciones 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 ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Para obtener más información, consulte [Etiquetado de los recursos de AWS](#).

variable de destino

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

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de

procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

[Consulte entorno.](#)

entrenamiento

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

puerta de enlace de tránsito

Un centro de tránsito de red que puede usar para interconectar sus VPCs redes con las locales. Para obtener más información, consulte [Qué es una pasarela de tránsito](#) en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

tareas indiferenciadas

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

entornos superiores

Ver [entorno](#).

V

succión

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

control de versión

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

Emparejamiento de VPC

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

carga de trabajo

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

flujo de trabajo

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

GUSANO

Mira, [escribe una vez, lee muchas](#).

WQF

Consulte el [marco AWS de calificación de la carga](#) de trabajo.

escribe una vez, lee muchas (WORM)

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

Z

ataque de día cero

Un ataque, normalmente de malware, que aprovecha una vulnerabilidad de [día cero](#).

vulnerabilidad de día cero

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

aviso de tiro cero

Proporcionar a un [LLM](#) instrucciones para realizar una tarea, pero sin ejemplos (imágenes) que puedan ayudar a guiarla. El LLM debe utilizar sus conocimientos previamente entrenados para realizar la tarea. La eficacia de las indicaciones cero depende de la complejidad de la tarea y de la calidad de las indicaciones. [Consulte también las indicaciones de 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 versión original de inglés, prevalecerá la versión en inglés.