



Ferramentas de monitoramento e alerta e melhores práticas do Amazon RDS
for MySQL e MariaDB

AWS Orientação prescritiva



AWS Orientação prescritiva: Ferramentas de monitoramento e alerta e melhores práticas do Amazon RDS for MySQL e MariaDB

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

Table of Contents

Introdução	1
Visão geral	3
Resultados de negócios desejados	4
Melhores práticas gerais	7
Ferramentas de monitoramento	9
Ferramentas incluídas no Amazon RDS	10
CloudWatch namespaces	10
CloudWatch alarmes e painéis	12
Insights de Performance do Amazon RDS	13
Monitoramento avançado	15
AWS Serviços adicionais	15
Ferramentas de monitoramento de terceiros	17
Prometheus e Grafana	17
Percona	19
Monitoramento da instância de banco	20
Métricas de insights de desempenho para instâncias de banco de dados	21
Carga de banco de dados	21
Dimensões	22
Métricas de contador	23
Estatísticas SQL	26
CloudWatch métricas para instâncias de banco de dados	27
Publicando métricas do Performance Insights em CloudWatch	28
Monitoramento do SO	29
Eventos, registros e trilhas de auditoria	36
Eventos do Amazon RDS	36
Registros do banco	40
Trilhas de auditoria	43
Exemplo	44
Adicional CloudTrail e CloudWatch Recursos de registros	47
Geração de alertas	48
Alarmes do CloudWatch	49
Regras do EventBridge	52
Especificando ações, ativando e desativando alarmes	54
Próximas etapas e recursos	55

Histórico do documento	56
Glossário	57
#	57
A	58
B	61
C	63
D	66
E	71
F	73
G	74
H	75
I	76
L	79
M	80
O	84
P	87
Q	90
R	90
S	93
T	97
U	98
V	99
W	99
Z	100
.....	ci

Ferramentas de monitoramento e alerta e melhores práticas para o Amazon RDS para MySQL e MariaDB

Igor Obradovic, Amazon Web Services (AWS)

Junho de 2023([histórico do documento](#))

O monitoramento de banco de dados é o processo de medir, rastrear e avaliar a disponibilidade, o desempenho e a funcionalidade de um banco de dados. As soluções de monitoramento e alerta ajudam as organizações a garantir que seus serviços de banco de dados e, portanto, seus aplicativos e cargas de trabalho associados sejam seguros, de alto desempenho, resilientes e eficientes. Na AWS, você pode coletar e analisar seus registros, métricas, eventos e rastreamentos de carga de trabalho para entender a integridade de sua carga de trabalho e obter insights das operações ao longo do tempo.

Você pode monitorar seus recursos para garantir que eles estejam funcionando conforme o esperado e para detectar e corrigir quaisquer problemas antes que eles afetem seus clientes. Você deve usar as métricas, registros, eventos e rastreamentos que você monitora para acionar alarmes quando os limites são ultrapassados.

Este guia descreve as ferramentas de observabilidade e monitoramento do banco de dados e as melhores práticas para bancos de dados do Amazon Relational Database Service (Amazon RDS). O guia se concentra nos bancos de dados MySQL e MariaDB, embora a maioria das informações também se aplique a outros mecanismos de banco de dados do Amazon RDS.

Este guia é para arquitetos de soluções, arquitetos de banco de dados, DBAs e idososDevOpsengenheiros e outros membros da equipe que se dedicam ao projeto, implementação e gerenciamento de soluções de monitoramento e observabilidade para suas cargas de trabalho de banco de dados em execução na nuvem da AWS.

Índice

- [Visão geral](#)
- [Melhores práticas gerais](#)
- [Ferramentas de monitoramento](#)
- [Monitoramento da instância de banco](#)
- [Monitoramento do SO](#)

- [Eventos, registros e trilhas de auditoria](#)
- [Geração de alertas](#)
- [Próximas etapas e recursos](#)

Visão geral

O monitoramento e o alerta estão incluídos em quatro pilares do Well-Architected AWS Framework.

- O [pilar de excelência operacional](#) prescreve que sua carga de trabalho deve ser projetada para incluir telemetria e monitoramento. AWS serviços como o [Amazon Relational Database Service \(Amazon RDS\)](#) fornecem as informações necessárias para que você entenda o estado interno da sua carga de trabalho (por exemplo, métricas, registros, eventos e rastreamentos). Ao operar seus bancos de dados do Amazon RDS, você desejará entender a integridade das instâncias de seus bancos de dados, detectar eventos operacionais e ser capaz de responder a eventos planejados e não planejados. A AWS fornece ferramentas de monitoramento que ajudam você a determinar quando os resultados organizacionais e comerciais estão em risco ou podem estar em risco, para que você possa tomar as medidas apropriadas no momento certo.
- O [pilar de eficiência de desempenho](#) prescreve que você deve monitorar o desempenho de seus recursos, como instâncias de banco de dados do Amazon RDS, reunindo, agregando e processando métricas relacionadas ao desempenho em tempo real. Você pode identificar a degradação do desempenho e corrigir os fatores, por exemplo, consultas SQL não otimizadas ou parâmetros de configuração inadequados, que a causaram. Você pode acionar alarmes automaticamente quando as medições estão fora dos limites esperados. Recomendamos que você use alarmes não apenas para notificações, mas também para iniciar ações automatizadas em resposta aos eventos detectados. Você pode avaliar as métricas coletadas em relação a limites predefinidos ou usar algoritmos de aprendizado de máquina para identificar comportamentos anômalos. Por exemplo, para detectar uma tendência de aumento na utilização da CPU, você pode coletar e analisar a `cpuUtilization.total` métrica durante um período de tempo. Alertar sobre essa anomalia de forma proativa, antes que a utilização da CPU atinja o limite máximo, pode ajudá-lo a corrigir o problema antes que ele afete seus clientes.
- O [pilar de confiabilidade](#) define o monitoramento e o alerta como essenciais para garantir que você atenda aos requisitos de disponibilidade. Sua solução de monitoramento deve ser capaz de detectar falhas de forma eficaz. Quando detecta problemas ou falhas, seu objetivo principal é alertar sobre esses problemas. Implementar práticas contínuas de observabilidade e monitoramento é fundamental para arquiteturas resilientes na nuvem. Para melhorar suas cargas de trabalho, você deve ser capaz de medi-las e entender seu estado e integridade. Os princípios de design para recuperação automática de uma falha, escalabilidade horizontal e provisionamento de capacidade dependem de serviços precisos de monitoramento e alerta.

- O [pilar de segurança](#) discute a detecção e a prevenção de alterações de configuração inesperadas ou indesejadas e de comportamentos inesperados. Você pode configurar suas [instâncias de banco de dados Amazon RDS for MySQL e MariaDB com o MariaDB Audit Plugin para registrar atividades do](#) banco de dados, como logins de usuários e operações específicas executadas no banco de dados. O plug-in armazena o registro da atividade do banco de dados em um arquivo de log, que pode ser integrado e importado para ferramentas de monitoramento e alerta. O arquivo de log é analisado em tempo real para detectar comportamentos inesperados ou suspeitos em seu banco de dados. Esse comportamento inesperado ou suspeito pode indicar que sua instância de banco de dados Amazon RDS foi comprometida, o que sinaliza riscos potenciais para sua empresa. Se a ferramenta de monitoramento detectar esse evento, ela ativará um alarme para iniciar uma resposta ao incidente de segurança, o que ajuda a lidar com atividades suspeitas e maliciosas.

Resultados de negócios desejados

A implementação das melhores práticas em mecanismos de monitoramento e alerta ajuda você a garantir uma infraestrutura de alto desempenho, resiliente, eficiente, segura e com custos otimizados para seus aplicativos e cargas de trabalho. Você pode usar ferramentas de observabilidade que coletam, armazenam e visualizam métricas, eventos, rastreamentos e registros em tempo real para observar e analisar o panorama geral da integridade e do desempenho de seus bancos de dados e, assim, evitar a degradação ou interrupção dos serviços de TI associados. Se a degradação não planejada ou a interrupção do serviço ainda ocorrerem, as ferramentas de monitoramento e alerta ajudarão você a detectar o problema em tempo hábil, escalar, reagir e investigar e resolver rapidamente. Uma solução abrangente de monitoramento e alerta para suas cargas de trabalho de banco de dados em nuvem ajuda você a alcançar os seguintes resultados comerciais:

- Melhore a experiência do cliente. Um serviço confiável melhora as experiências de seus clientes. Os bancos de dados geralmente são um componente essencial dos serviços digitais, como aplicativos móveis e da web, streaming de mídia, pagamentos, APIs business-to-business (B2B) e serviços de integração. Se você puder monitorar e configurar alertas em seus bancos de dados para detectar problemas rapidamente, investigá-los com eficiência e corrigi-los o mais rápido possível para minimizar o tempo de inatividade e outras interrupções, poderá aprimorar a disponibilidade, a segurança e o desempenho do serviço digital para seus clientes.
- Conquiste a confiança do cliente. Um melhor desempenho e uma experiência de usuário mais suave ajudam você a conquistar a confiança de seus clientes, o que pode resultar em mais negócios em sua plataforma. Por exemplo, um provedor de serviços de processamento de

pagamentos que oferece um serviço on-line confiável pode esperar alta confiança e fidelidade do cliente, o que resulta em mais clientes e melhor retenção, aumento nas transações faturáveis e serviços novos e inovadores que geram mais receita.

- Evite perdas financeiras. Qualquer tempo de inatividade inesperado em sua infraestrutura de banco de dados pode afetar as transações comerciais que seus clientes realizam usando seu aplicativo. Isso pode levar a perdas financeiras substanciais em alguns casos. A violação dos contratos de nível de serviço (SLAs) pode resultar na perda da confiança do cliente e, conseqüentemente, na perda de receita. Também pode se tornar uma base legal para testes caros, nos quais os clientes podem exigir compensação com base em seus contratos de responsabilidade e garantia. De acordo com um [estudo da Atlassian Corporation](#), uma empresa de software, os custos médios da interrupção do serviço estão na faixa de \$140 mil a \$540 mil por hora, dependendo do tipo e tamanho da empresa. Um ambiente de banco de dados estável é fundamental para evitar interrupções prolongadas e perda de negócios.
- Expanda o valor. Mecanismos de monitoramento e alerta podem ajudá-lo a projetar, desenvolver e operar um serviço digital altamente disponível, resiliente, confiável, de alto desempenho, econômico e seguro, mas isso é só o começo. Você desejará que sua organização cresça e prospere com o tempo, aprimore as cargas de trabalho existentes na nuvem e introduza novos serviços. Novos serviços fornecem valor adicional aos seus clientes e mais receita à sua empresa, criando um efeito inversor no crescimento da sua empresa.
- Melhore a produtividade do desenvolvedor. Desenvolvedores que são produtivos e eficientes, e que não encontram problemas e gargalos em suas tarefas de desenvolvimento, podem entregar produtos de alta qualidade em menos tempo. No entanto, a engenharia de software e as operações de TI geralmente têm desafios complexos, e essa complexidade aumenta com a escala das cargas de trabalho e suas arquiteturas. Para analisar o desempenho e a consistência em aplicativos distribuídos, os desenvolvedores precisam de ferramentas que possam fornecer métricas e rastreamentos correlacionados. Eles ajudam a identificar artefatos de código e componentes de infraestrutura com defeito o mais rápido possível e ajudam a determinar os impactos nos usuários finais. O conjunto certo de ferramentas de monitoramento e alerta pode ajudar os desenvolvedores a programar e testar de forma melhor e mais rápida.
- Melhore a eficácia e a eficiência operacionais. Quando você opera cargas de trabalho na nuvem em grande escala, até mesmo uma pequena porcentagem de melhorias no desempenho pode resultar em economias de milhões de dólares. Ao monitorar seus bancos de dados e analisar métricas, eventos, registros e rastreamentos, você pode entender e prever suas futuras necessidades de capacidade e aproveitar as economias de custo disponíveis na nuvem da AWS.

Compreender as cargas de trabalho e a saúde operacional do Amazon RDS pode ajudá-lo a responder a eventos, corrigir problemas e planejar melhorias.

Melhores práticas gerais

As melhores práticas a seguir ajudam você a obter visibilidade suficiente sobre a integridade de sua carga de trabalho do Amazon RDS e a tomar as ações apropriadas em resposta a eventos operacionais e dados de monitoramento.

- **Identifique os KPIs.** Identifique os principais indicadores de desempenho (KPIs) com base nos resultados comerciais desejados. Avalie os KPIs para determinar o sucesso da carga de trabalho. Por exemplo, se o seu negócio principal é o comércio eletrônico, um dos resultados comerciais desejados pode ser que sua loja virtual esteja disponível 24 horas por dia, 7 dias por semana, para que seus clientes façam suas compras. Para alcançar esse resultado comercial, você define o KPI de disponibilidade para o banco de dados de back-end do Amazon RDS que seu aplicativo de loja virtual usa e define o KPI básico como 99,99% semanalmente. Avaliar o KPI de disponibilidade real em relação ao valor básico ajuda a determinar se você está atingindo a disponibilidade de banco de dados desejada de 99,99% e, assim, alcançando o resultado comercial de ter um serviço 24 horas por dia, 7 dias por semana.
- **Defina as métricas da carga de trabalho.** Defina métricas de carga de trabalho para medir as quantidades e qualidades de sua carga de trabalho do Amazon RDS. Avalie as métricas para determinar se a carga de trabalho está alcançando os resultados desejados e para entender a integridade da carga de trabalho. Por exemplo, para avaliar o KPI de disponibilidade da sua instância de banco de dados Amazon RDS, você deve medir métricas como tempo de atividade e tempo de inatividade da instância de banco de dados. Em seguida, você pode usar essas métricas para calcular o KPI de disponibilidade da seguinte forma:

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

As métricas representam conjuntos de pontos de dados ordenados no tempo. As métricas também podem incluir dimensões, que são úteis na categorização e análise.

- **Colete e analise métricas de carga de trabalho.** O Amazon RDS gera métricas e registros diferentes, dependendo da sua configuração. Alguns deles representam eventos, contadores ou estatísticas da instância de banco de dados, como `comodb.Cache.innoDB_buffer_pool_hits`. Outras métricas vêm do sistema operacional, como `memory.Total`, que mede a quantidade total de memória da instância hospedeira do Amazon Elastic Compute Cloud (Amazon EC2). A ferramenta de monitoramento deve realizar análises regulares e proativas das métricas coletadas para identificar tendências e determinar se alguma resposta apropriada é necessária.

- Estabeleça linhas de base de métricas de carga de trabalho. Estabeleça linhas de base para métricas para definir os valores esperados e identificar limites bons ou ruins. Por exemplo, você pode definir a linha de base para `ReadIOPS` de até 1.000 em operações normais de banco de dados. Em seguida, você pode usar essa linha de base para comparação e identificar a utilização excessiva. Se suas novas métricas mostrarem consistentemente que as IOPS de leitura estão na faixa de 2.000 a 3.000, você identificou um desvio que pode desencadear uma resposta para investigação, intervenção e melhoria.
- Alerta quando os resultados da carga de trabalho estiverem em risco. Quando você determinar que o resultado do negócio está em risco, emita um alerta. Você pode então resolver os problemas de forma proativa, antes que eles afetem seus clientes, ou mitigar o impacto do incidente em tempo hábil.
- Identifique os padrões de atividade esperados para sua carga de trabalho. Com base em suas linhas de base de métricas, estabeleça padrões de atividade da carga de trabalho para identificar comportamentos inesperados e responder com as ações apropriadas, se necessário. AWS fornece [ferramentas de monitoramento](#) que aplicam algoritmos estatísticos e de aprendizado de máquina para analisar métricas e detectar anomalias.
- Alerta quando forem detectadas anomalias na carga de trabalho. Quando forem detectadas anomalias nas operações das cargas de trabalho do Amazon RDS, emita um alerta para que você possa responder com as ações apropriadas, se necessário.
- Analise e revise KPIs e métricas. Confirme se seus bancos de dados do Amazon RDS atendem aos requisitos definidos e identifique áreas de possíveis melhorias para alcançar suas metas de negócios. Valide a eficácia das métricas medidas e dos KPIs avaliados e revise-os, se necessário. Por exemplo, digamos que você defina um KPI para o número ideal de conexões simultâneas de banco de dados e monitore métricas relacionadas a conexões tentadas e falhadas, bem como aos segmentos de usuário que foram criados e estão em execução. Você pode ter mais conexões de banco de dados do que aquelas definidas pela linha de base do KPI. Ao analisar suas métricas atuais, você pode detectar o resultado, mas talvez não consiga determinar a causa raiz. Nesse caso, você deve revisar suas métricas e incluir medidas adicionais de monitoramento, como contadores para fechaduras de mesa. As novas métricas ajudariam a determinar se o aumento do número de conexões de banco de dados é causado por bloqueios de tabela inesperados.

Ferramentas de monitoramento

Recomendamos que você use ferramentas de observabilidade, monitoramento e alerta para:

- Obtenha insights sobre o desempenho do seu ambiente Amazon RDS
- Detecte comportamentos inesperados e suspeitos
- Planeje a capacidade e tome decisões informadas sobre a alocação de instâncias do Amazon RDS
- Analise métricas e registros para prever possíveis problemas de forma proativa
- Gere alertas quando os limites forem violados para solucionar e resolver problemas antes que seus usuários sejam afetados

Você tem diferentes opções e soluções para escolher, incluindo ferramentas e serviços de observabilidade e monitoramento nativos da nuvem fornecidos pela AWS; soluções de software gratuitas de código aberto; e soluções comerciais de terceiros para monitorar instâncias de banco de dados do Amazon RDS. Algumas dessas ferramentas são discutidas nas seções a seguir.

Para determinar qual ferramenta atende melhor às suas necessidades, compare os recursos e capacidades de cada ferramenta com os requisitos da sua organização. Também recomendamos que você avalie as ferramentas quanto à facilidade de implantação, configuração e integração, atualizações e manutenção de software, método de implantação (por exemplo, hardware ou sem servidor), licenciamento, preço e quaisquer outros fatores específicos da sua organização.

Seções

- [Ferramentas incluídas no Amazon RDS](#)
- [CloudWatch namespaces](#)
- [CloudWatch alarmes e painéis](#)
- [Insights de Performance do Amazon RDS](#)
- [Monitoramento avançado](#)
- [AWS Serviços adicionais](#)
- [Ferramentas de monitoramento de terceiros](#)

Ferramentas incluídas no Amazon RDS

O Amazon Relational Database Service (Amazon RDS) é um serviço de banco de dados gerenciado na nuvem da AWS. Como o Amazon RDS é um serviço gerenciado, ele libera você da maioria das tarefas de gerenciamento, como backups de banco de dados, instalações de sistema operacional (SO) e software de banco de dados, aplicação de patches de sistemas operacionais e software, configuração de alta disponibilidade, ciclo de vida de hardware e operações de data center. AWS também fornece um conjunto abrangente de ferramentas que permitem criar uma solução completa de [observabilidade](#) para suas instâncias de banco de dados Amazon RDS.

Algumas das ferramentas de monitoramento estão incluídas, pré-configuradas e habilitadas automaticamente no serviço Amazon RDS. Duas ferramentas automatizadas estão disponíveis para você assim que você inicia sua nova instância do Amazon RDS:

- O status da instância do Amazon RDS fornece detalhes sobre a saúde atual da sua instância de banco de dados. Por exemplo, os códigos de status incluem Disponível, Parado, Criação, Backup e Falha. Você pode usar o console do Amazon RDS, o AWS Command Line Interface (AWS CLI) ou a API do Amazon RDS para ver o status da instância. Para obter mais informações, consulte [Visualizar o status da instância de banco de dados do Amazon RDS](#) na documentação do Amazon RDS.
- As recomendações do Amazon RDS fornecem recomendações automatizadas para instâncias de banco de dados, réplicas de leitura e grupos de parâmetros de banco de dados. Essas recomendações são fornecidas analisando o uso, os dados de desempenho e a configuração da instância de banco de dados e são fornecidas como orientação. Por exemplo, a recomendação da versão desatualizada do Engine sugere que suas instâncias de banco de dados não estão executando a versão mais recente do software de banco de dados e que você deve atualizar sua instância de banco de dados para se beneficiar das correções de segurança e outras melhorias mais recentes. Para obter mais informações, consulte [Visualização das recomendações do Amazon RDS](#) na documentação do Amazon RDS.

CloudWatch namespaces

O Amazon RDS se integra à [Amazon CloudWatch](#), que é um serviço de monitoramento e alerta para recursos e aplicativos em nuvem executados na AWS. O Amazon RDS coleta automaticamente métricas, arquivos de log, rastreamentos e eventos sobre a operação, a utilização, o desempenho

e a integridade das instâncias de banco de dados e os envia CloudWatch para armazenamento, análise e alertas a longo prazo.

O Amazon RDS for MySQL e o Amazon RDS for MariaDB publicam automaticamente um conjunto CloudWatch padrão de métricas em intervalos de um minuto, sem custo adicional. Essas métricas são coletadas em dois namespaces, que são contêineres para métricas:

- O [namespace AWS/RDS inclui métricas](#) em nível de instância de banco de dados. Os exemplos incluem BinLogDiskUsage (a quantidade de espaço em disco ocupado pelos registros binários), CPUUtilization (a porcentagem de utilização da CPU), DatabaseConnections (o número de conexões de rede do cliente com a instância de banco de dados) e muito mais.
- O [namespace AWS/Usage inclui métricas de uso em nível de conta, que são usadas para determinar se você está operando dentro das cotas de serviço do Amazon RDS](#). Os exemplos incluem DBInstances (o número de instâncias de banco de dados em sua conta ou região da AWS), DBSubnetGroups (o número de grupos de sub-redes de banco de dados em sua AWS conta ou região) e ManualSnapshots (o número de snapshots de banco de dados criados manualmente em sua AWS conta ou região).

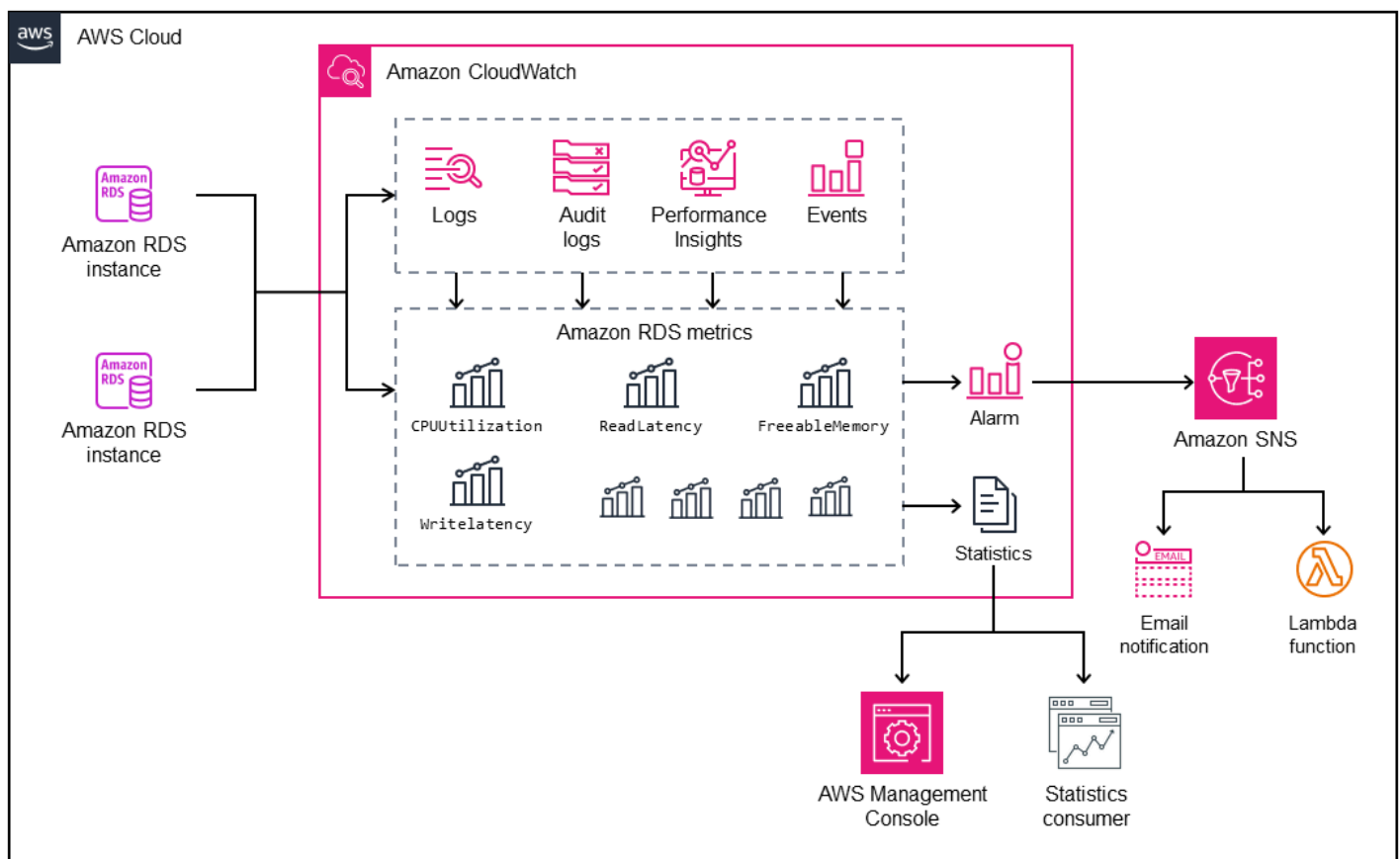
CloudWatch retém os dados métricos da seguinte forma:

- 3 horas: métricas personalizadas de alta resolução com um período inferior a 60 segundos são mantidas por 3 horas. Depois de 3 horas, os pontos de dados são agregados em métricas de período de 1 minuto e mantidos por 15 dias.
- 15 dias: os pontos de dados com um período de 60 segundos (1 minuto) são retidos por 15 dias. Após 15 dias, os pontos de dados são agregados em métricas de período de 5 minutos e mantidos por 63 dias.
- 63 dias: os pontos de dados com um período de 300 segundos (5 minutos) são retidos por 63 dias. Após 63 dias, os pontos de dados são agregados em métricas de período de 1 hora e mantidos por 15 meses.
- 15 meses: pontos de dados com um período de 3.600 segundos (1 hora) estão disponíveis por 15 meses (455 dias).

Para obter mais informações, consulte [Métricas](#) na CloudWatch documentação.

CloudWatch alarmes e painéis

Você pode usar [CloudWatch os alarmes da Amazon](#) para observar uma métrica específica do Amazon RDS durante um período de tempo. Por exemplo, você pode monitorar `FreeStorageSpace`, em seguida, realizar uma ou mais ações se o valor da métrica ultrapassar o limite definido. Se você definir o limite para 250 MB e o espaço de armazenamento gratuito for 200 MB (menos do que o limite), o alarme será ativado e poderá acionar uma ação para provisionar automaticamente armazenamento adicional para a instância de banco de dados Amazon RDS. O alarme também pode enviar uma notificação por SMS ao DBA usando o Amazon Simple Notification Service (Amazon SNS). O diagrama a seguir ilustra esse processo.



CloudWatch também fornece [painéis](#), que você pode usar para criar, personalizar, interagir e salvar visualizações personalizadas (gráficos) das métricas. Você também pode usar o [CloudWatch Logs Insights](#) para criar um painel para monitorar o registro de consultas lentas e o registro de erros e para receber alertas se um padrão específico for detectado nesses registros. A tela a seguir mostra um exemplo de CloudWatch painel.

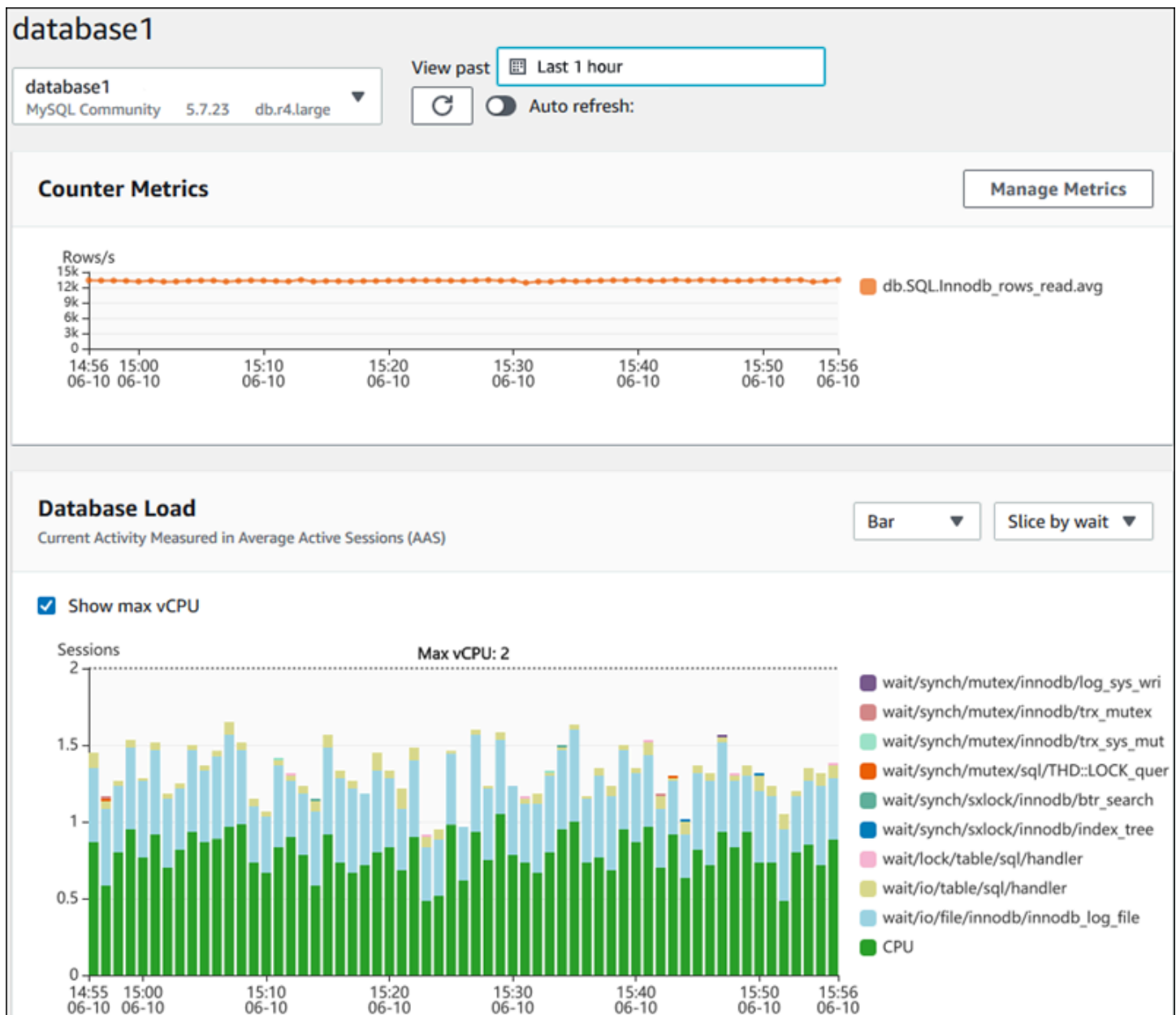
The screenshot displays the Amazon RDS Performance Insights dashboard for a MySQL instance named 'demo-mysql-dev'. The dashboard is divided into several sections:

- Slow queries with detailed info:** A table listing the top 10 slowest queries. Columns include #, Time, User, Id, Query_time, Lock_time, Rows_sent, Rows_examined, timestamp, and query. The queries are mostly 'select' statements involving 'mtb_data' and 'mtb' tables.
- Top Slow Queries sorted by Query Time:** A table listing the top 10 slowest queries sorted by query time. Columns include #, Time, Query_time, and Query. The queries are similar to the ones in the first table.
- Top 200 lines of Error Log:** A table listing the top 200 lines of the error log. Columns include #, @message, and the error message itself. The messages are related to database connections and events.

The dashboard also includes a sidebar with various navigation options such as CloudWatch, Dashboards, Alarms, Billing, Logs, Log groups, Insights, Metrics, Events, Rules, Event Buses, ServiceLens, Service Map, Traces, Container Insights, Resources, Performance Monitoring, Synthetics, Canaries, Contributor Insights, and Settings.

Insights de Performance do Amazon RDS

[O Amazon RDS Performance Insights](#) é uma ferramenta de ajuste e monitoramento de desempenho de banco de dados que expande os recursos de monitoramento do Amazon RDS. Ele ajuda você a analisar o desempenho do seu banco de dados visualizando a carga da instância de banco de dados e filtrando a carga por esperas, instruções SQL, hosts ou usuários. A ferramenta combina várias métricas em um único gráfico interativo que ajuda a identificar o tipo de gargalo que sua instância de banco de dados pode ter, como esperas de bloqueio, alto consumo de CPU ou latência de E/S, e determinar quais instruções SQL estão criando o gargalo. A tela a seguir mostra um exemplo de visualização.



Você precisa [ativar o Performance Insights](#) durante o processo de criação da instância de banco de dados para coletar métricas para as instâncias de banco de dados do Amazon RDS em sua conta. O nível gratuito inclui sete dias de histórico de dados de desempenho e um milhão de solicitações de API por mês. Opcionalmente, você pode comprar períodos de retenção mais longos. Para obter informações completas sobre custos, consulte [Definição de preço do Performance Insights](#).

Para obter informações sobre como você pode usar o Performance Insights para monitorar suas instâncias de banco de dados, consulte a seção de [monitoramento de instâncias de banco](#) de dados mais adiante neste guia.

O Performance Insights [publica automaticamente métricas em CloudWatch](#). Além de usar a ferramenta Performance Insights, você pode aproveitar os recursos adicionais que ela CloudWatch fornece. Você pode examinar as métricas do Performance Insights usando o CloudWatch console AWS CLI, o ou a CloudWatch API. Você também pode adicionar CloudWatch alarmes, como acontece com qualquer outra métrica. Por exemplo, talvez você queira acionar uma notificação por SMS para DBAs ou tomar uma ação corretiva se a DBLoad métrica ultrapassar o valor limite definido. Você também pode adicionar as métricas do Performance Insights aos seus CloudWatch painéis existentes.

Monitoramento avançado

O [monitoramento aprimorado](#) é uma ferramenta que captura métricas em tempo real para o sistema operacional (OS) no qual sua instância de banco de dados Amazon RDS é executada. Essas métricas fornecem granularidade de até um segundo para CPU, memória, processos do Amazon RDS e do sistema operacional, sistema de arquivos e dados de E/S de disco, entre outros. Você pode acessar e analisar essas métricas no [console do Amazon RDS](#). Assim como no Performance Insights, as métricas de monitoramento aprimorado são fornecidas pelo Amazon RDS para CloudWatch, onde você pode se beneficiar de recursos adicionais, como a preservação a longo prazo de métricas para análise, a criação de filtros de métricas, a exibição de gráficos no CloudWatch painel e a configuração de alarmes. Por padrão, o monitoramento aprimorado é desativado quando você cria uma nova instância de banco de dados Amazon RDS. Você pode [ativar](#) o recurso ao criar ou modificar uma instância de banco de dados. O preço é baseado na quantidade de dados transferidos do Amazon RDS para o CloudWatch Logs e nas taxas de armazenamento. Dependendo da granularidade e do número de instâncias de banco de dados em que o monitoramento aprimorado está ativado, parte dos dados de monitoramento pode ser incluída no nível gratuito de CloudWatch registros. Para obter detalhes completos sobre preços, consulte [Amazon CloudWatch Pricing](#). Para obter mais informações sobre a ferramenta, consulte a [documentação do Amazon RDS](#) e as perguntas frequentes sobre [monitoramento aprimorado](#).

AWS Serviços adicionais

AWS fornece vários serviços de suporte, que também se integram ao Amazon RDS e CloudWatch melhoram ainda mais a observabilidade de seus bancos de dados. Isso inclui Amazon EventBridge, Amazon CloudWatch Logs AWS CloudTrail e.

- EventBridgeA [Amazon](#) é um barramento de eventos sem servidor que pode receber, filtrar, transformar, rotear e entregar eventos de seus aplicativos e AWS recursos, incluindo suas

instâncias de banco de dados Amazon RDS. Um evento do Amazon RDS indica uma mudança no ambiente do Amazon RDS. Por exemplo, quando uma instância de banco de dados muda seu status de Disponível para Parada, o Amazon RDS gera o evento `RDS-EVENT-0087` / `The DB instance has been stopped`. O Amazon RDS entrega eventos para CloudWatch eventos e quase EventBridge em tempo real. Usando EventBridge and CloudWatch Events, você pode definir regras para enviar alertas sobre eventos específicos de interesse do Amazon RDS e automatizar ações a serem tomadas quando um evento corresponder à regra. Várias metas estão disponíveis em resposta a um evento, como uma AWS Lambda função que pode realizar uma ação corretiva ou um tópico do Amazon SNS que pode enviar um e-mail ou SMS para notificar DBAs DevOps ou engenheiros sobre o evento.

- O [Amazon CloudWatch Logs](#) é um serviço que centraliza o armazenamento de arquivos de log de todos os seus aplicativos, sistemas e AWS serviços, incluindo instâncias de banco de dados Amazon RDS for MySQL e MariaDB e. AWS CloudTrail Se você [habilitar](#) o recurso para suas instâncias de banco de dados, o Amazon RDS publicará automaticamente os seguintes registros no Logs: CloudWatch
 - Log de erros
 - Log de consultas lentas
 - Log geral
 - Log de auditoria

Você pode usar o CloudWatch Logs Insights para consultar e analisar os dados do registro. O recurso inclui uma linguagem de consulta específica que ajuda você a pesquisar eventos de log que correspondam aos padrões definidos por você. Por exemplo, você pode rastrear a corrupção de tabelas em sua instância de banco de dados MySQL monitorando o arquivo de log de erros em busca do seguinte padrão: `"ERROR 1034 (HY000): Incorrect key file for table '*'; try to repair it OR Table * is marked as crashed"` Os dados de registro filtrados podem ser convertidos em CloudWatch métricas. Em seguida, você pode usar as métricas para criar painéis com gráficos ou dados tabulares ou definir um alarme se o valor limite definido for violado. Isso é particularmente útil ao usar o registro de auditoria, pois você pode monitorar, enviar alertas e tomar ações corretivas automaticamente se algum comportamento inesperado ou suspeito for detectado. Você pode acessar e gerenciar registros do banco de dados usando o AWS Management Console AWS CLI, a API do Amazon RDS ou o AWS SDK for CloudWatch Logs.

- [AWS CloudTrail](#) registra e monitora continuamente a atividade do usuário e da API em sua conta da AWS. Ele ajuda você com auditoria, monitoramento de segurança e solução

de problemas operacionais de suas instâncias de banco de dados Amazon RDS for MySQL ou MariaDB. CloudTrail está integrado ao Amazon RDS. Todas as ações podem ser registradas e CloudTrail fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Amazon RDS. Por exemplo, quando um usuário cria uma nova instância de banco de dados Amazon RDS, um evento é detectado e o log inclui informações sobre a ação solicitada ("eventName": "CreateDBInstance"), a data e a hora da ação ("eventTime": "2022-07-30T22:14:06Z"), os parâmetros da solicitação ("requestParameters": {"dbInstanceIdentifier": "test-instance", "engine": "mysql", "dbInstanceClass": "db.m6g.large"}) e assim por diante. Os eventos registrados CloudTrail incluem chamadas do console do Amazon RDS e chamadas de código que usa a API do Amazon RDS.

Ferramentas de monitoramento de terceiros

Em alguns cenários, além do conjunto completo de ferramentas de monitoramento e observabilidade nativas da nuvem que fornece AWS para o Amazon RDS, talvez você queira usar ferramentas de monitoramento de outros fornecedores de software. Esses cenários incluem implantações híbridas, nas quais você pode ter vários bancos de dados em execução em seu data center local e outro conjunto de bancos de dados em execução no. Nuvem AWS Se você já estabeleceu sua solução corporativa de observabilidade, talvez queira continuar usando suas ferramentas existentes e estendê-las às suas implantações na nuvem da AWS. O desafio de configurar uma solução de monitoramento terceirizada geralmente está nas salvaguardas impostas pelo Amazon RDS como um serviço gerenciado na nuvem. Por exemplo, você não pode instalar o software do agente no sistema operacional host que executa a instância de banco de dados, porque o acesso à máquina host do banco de dados é negado. No entanto, você pode integrar várias soluções de monitoramento de terceiros com o Amazon RDS, construindo sobre outros Nuvem AWS serviços. CloudWatch Por exemplo, métricas, registros, eventos e rastreamentos do Amazon RDS podem ser exportados e depois importados para a ferramenta de monitoramento terceirizada para análise, visualização e alertas adicionais. Algumas dessas soluções de terceiros incluem Prometheus, Grafana e Percona.

Prometheus e Grafana

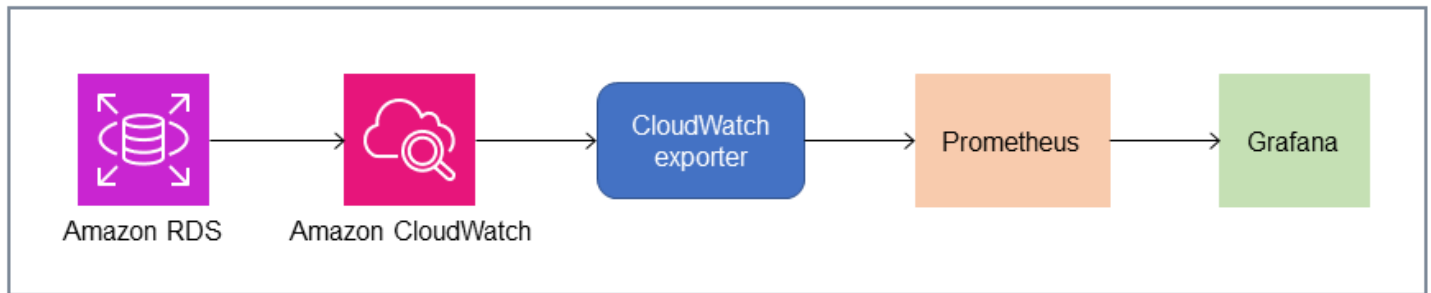
O [Prometheus](#) é [uma](#) solução de monitoramento de código aberto que coleta métricas de alvos configurados em determinados intervalos. É uma solução de monitoramento de uso geral que pode monitorar qualquer aplicativo ou serviço. Quando você monitora instâncias de banco de dados do Amazon RDS, CloudWatch coleta as métricas do Amazon RDS. As métricas são então exportadas

para o servidor Prometheus usando um exportador de código aberto, como o exportador YACE ou o Exporter. CloudWatch

- O [exportador YACE](#) otimiza as tarefas de exportação de dados recuperando várias métricas em uma única solicitação à API. CloudWatch Depois que as métricas são armazenadas no servidor Prometheus, o servidor avalia as expressões de regras e pode gerar alertas quando condições especificadas são observadas.
- [CloudWatch O Exporter](#) é oficialmente mantido pela Prometheus. Ele recupera CloudWatch métricas por meio da CloudWatch API e as armazena no servidor Prometheus em um formato compatível com o Prometheus, usando solicitações da API REST para o endpoint HTTP.

Ao escolher um exportador, projetar seu modelo de implantação e configurar instâncias do exportador, considere e [CloudWatchCloudWatch registre as](#) cotas de serviço e API, pois a exportação de métricas CloudWatch para um servidor Prometheus é implementada sobre a API. CloudWatch Por exemplo, implantar várias instâncias do CloudWatch Exporter em uma única Conta da AWS região para monitorar centenas de instâncias de banco de dados do Amazon RDS pode resultar em um erro de limitação () ThrottlingException erros de código 400. Para superar essas limitações, considere usar o exportador YACE, que é otimizado para coletar até 500 métricas diferentes em uma única solicitação. Além disso, para implantar um grande número de instâncias de banco de dados do Amazon RDS, você deve considerar o uso de [várias Contas da AWS](#), em vez de centralizar a carga de trabalho em uma única Conta da AWS e limitar o número de instâncias do exportador em cada uma. Conta da AWS

[Os alertas são gerados pelo servidor Prometheus e gerenciados pelo Alertmanager.](#) Essa ferramenta se encarrega de deduplicar, agrupar e rotear alertas para o destinatário correto, como e-mail, SMS ou Slack, ou iniciar uma ação de resposta automática. Outra ferramenta [de código aberto](#) chamada [Grafana](#) exibe visualizações dessas métricas. O Grafana fornece widgets de visualização avançados, como gráficos avançados, painéis dinâmicos e recursos de análise, como consultas ad-hoc e detalhamento dinâmico. Ele também pode pesquisar e analisar registros e inclui recursos de alerta para avaliar continuamente métricas e registros e enviar notificações quando os dados corresponderem às regras de alerta.



Percona

O [Percona Monitoring and Management \(PMM\)](#) é uma solução gratuita de monitoramento, gerenciamento e observabilidade de banco de dados de [código aberto](#) para MySQL e MariaDB. O PMM coleta milhares de métricas de desempenho de instâncias de banco de dados e seus hosts. Ele fornece uma interface de usuário da web para visualizar dados em painéis e recursos adicionais, como consultores automáticos para avaliações de integridade do banco de dados. Você pode usar o PMM para monitorar o Amazon RDS. No entanto, o cliente PMM (agente) não está instalado nos hosts subjacentes das instâncias de banco de dados do Amazon RDS, porque não tem acesso aos hosts. Em vez disso, a ferramenta se conecta às instâncias de banco de dados do Amazon RDS, consulta estatísticas do servidor `INFORMATION_SCHEMA`, esquema de sistemas e esquema de desempenho e usa a CloudWatch API para adquirir métricas, registros, eventos e rastreamentos. O PMM exige uma chave de acesso do usuário AWS Identity and Access Management (IAM) (função do IAM) e descobre automaticamente as instâncias de banco de dados do Amazon RDS que estão disponíveis para monitoramento. A ferramenta PMM tem um perfil para monitoramento de banco de dados e coleta mais métricas específicas do banco de dados do que o Prometheus. Para usar o [painel do PMM Query Analytics](#), você deve configurar o Esquema de Desempenho como a fonte da consulta, pois o agente do Query Analytics não está instalado para o Amazon RDS e não consegue ler o log de consultas lentas. Em vez disso, ele consulta diretamente as `performance_schema` instâncias de banco de dados MySQL e MariaDB para obter métricas. Uma das características proeminentes do PMM é sua [capacidade de alertar](#) e aconselhar DBAs sobre problemas que a ferramenta identifica em seus bancos de dados. O PMM oferece conjuntos de verificações que podem detectar ameaças comuns à segurança, degradação do desempenho, perda e corrupção de dados.

Além dessas ferramentas, há várias soluções comerciais de observabilidade e monitoramento disponíveis no mercado que podem ser integradas ao Amazon RDS. [Os exemplos incluem monitoramento de banco de dados Datadog, monitoramento do Dynatrace Amazon RDS e monitoramento de banco de dados. AppDynamics](#)

Monitoramento da instância de banco

UMA [instância de banco de dados](#) é o componente básico do Amazon RDS. É um ambiente de banco de dados isolado que é executado na nuvem. Para bancos de dados MySQL e MariaDB, a instância de banco de dados é a [mysqld](#) programa, também conhecido como servidor MySQL, que inclui vários segmentos e componentes, como o analisador SQL, o otimizador de consultas, o manipulador de encadeamento/conexão, variáveis de sistema e status e um ou mais mecanismos de armazenamento conectáveis. Cada mecanismo de armazenamento foi projetado para oferecer suporte a um caso de uso especializado. O mecanismo de armazenamento padrão e recomendado é [InnoDB](#), que é um mecanismo de banco de dados transacional, de uso geral e relacional que está em conformidade com o modelo de atomicidade, consistência, isolamento, durabilidade (ACID). Recursos do InnoDB [estruturas na memória](#) (buffer pool, buffer de alteração, índice de hash adaptativo, buffer de log), bem como [estruturas em disco](#) (espaços de tabela, tabelas, índices, registro de desfazer, refazer log, arquivos de buffer de gravação dupla). Para garantir que seu banco de dados cumpra rigorosamente o modelo ACID, o [O mecanismo de armazenamento InnoDB implementa vários recursos](#) para proteger seus dados, incluindo transações, confirmação, reversão, recuperação de falhas, bloqueio em nível de linha e controle de simultaneidade multiversão (MVCC).

Todos esses componentes internos de uma instância de banco de dados trabalham em conjunto para ajudar a manter a disponibilidade, a integridade e a segurança de seus dados no nível de desempenho esperado e satisfatório. Dependendo da sua carga de trabalho, cada componente e recurso pode impor demandas de recursos aos subsistemas de CPU, memória, rede e armazenamento. Quando um aumento na demanda por um recurso específico excede a capacidade provisionada ou os limites de software desse recurso (impostos pelos parâmetros de configuração ou pelo design do software), a instância de banco de dados pode sofrer degradação do desempenho ou total indisponibilidade e corrupção. Portanto, é fundamental medir e monitorar esses componentes internos, compará-los com os valores de linha de base definidos e gerar alertas se os valores monitorados se desviarem dos valores esperados.

Conforme descrito anteriormente, você pode usar diferentes [ferramentas](#) para monitorar suas instâncias do MySQL e do MariaDB. Recomendamos que você use o Amazon RDS Performance Insights e CloudWatch ferramentas para monitoramento e alerta, porque essas ferramentas são integradas ao Amazon RDS, reúnem métricas de alta resolução, apresentam as informações de desempenho mais recentes quase em tempo real e geram alarmes.

Independentemente da sua ferramenta de monitoramento preferida, recomendamos que você [ative o Esquema de Desempenho](#) em suas instâncias de banco de dados MySQL e MariaDB.

O [Esquema de desempenho](#) é um recurso opcional para monitorar a operação do servidor MySQL (a instância de banco de dados) em um nível baixo e foi projetado para ter um impacto mínimo no desempenho geral do banco de dados. Você pode gerenciar esse recurso usando `performance_schema` parâmetro. Embora esse parâmetro seja opcional, você deve usá-lo para coletar métricas de alta resolução (um segundo) por SQL, métricas de sessão ativa, eventos de espera e outras informações detalhadas de monitoramento de baixo nível, que são coletadas pelo Amazon RDS Performance Insights.

Seções

- [Métricas de insights de desempenho para instâncias de banco de dados](#)
- [CloudWatch métricas para instâncias de banco de dados](#)
- [Publicando métricas do Performance Insights em CloudWatch](#)

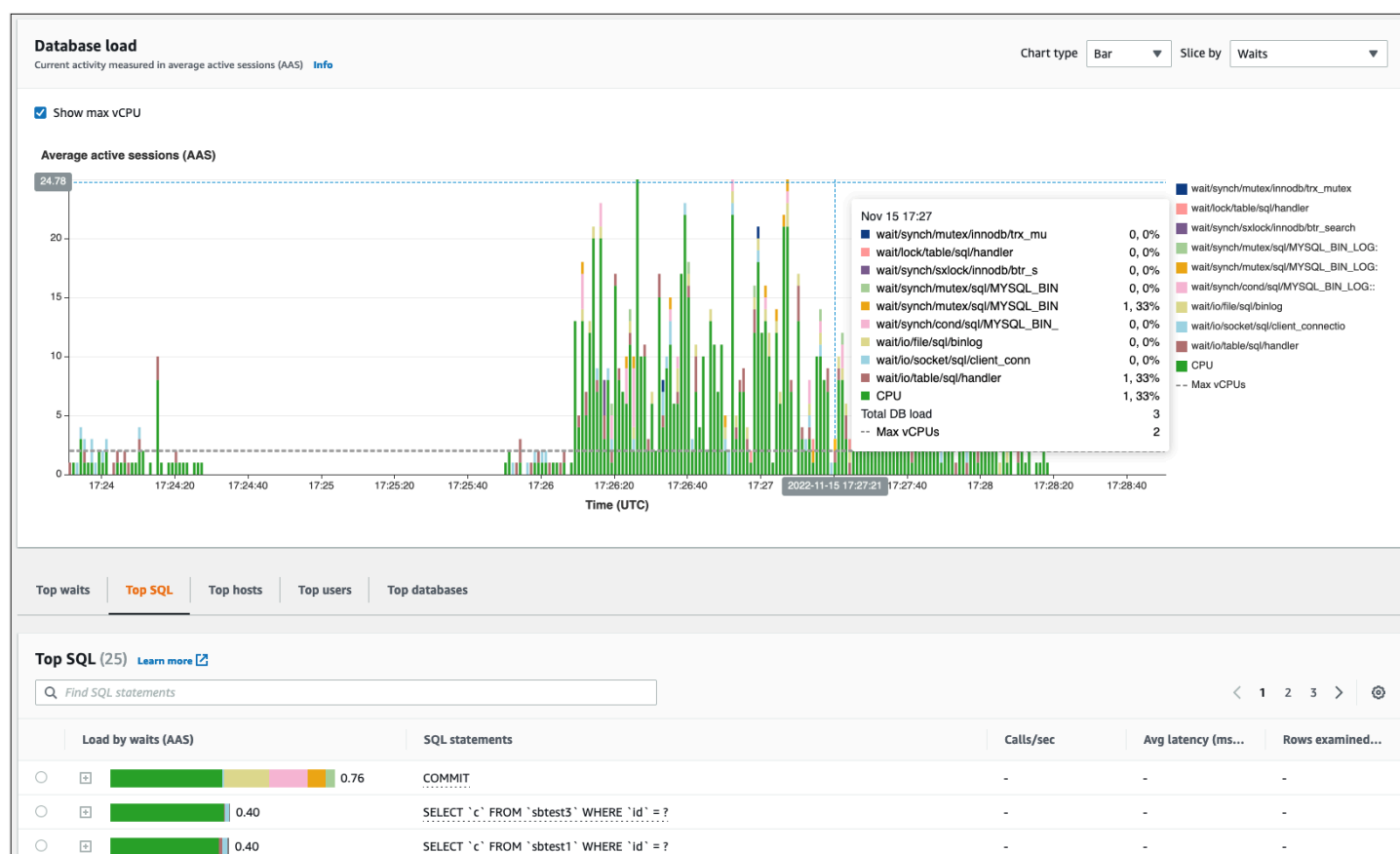
Métricas de insights de desempenho para instâncias de banco de dados

O Performance Insights monitora diferentes tipos de métricas, conforme discutido nas seções a seguir.

Carga de banco de dados

Carga do banco de dados (DBLoad) é uma métrica chave no Performance Insights que mede o nível de atividade em seu banco de dados. Ele é coletado a cada segundo e publicado automaticamente na AmazonCloudWatch. Ela representa a atividade da instância de banco de dados em sessões ativas médias (AAS), que é o número de sessões que estão executando consultas SQL simultaneamente. ODBLoada métrica é diferente de outras métricas de séries temporais, pois pode ser interpretada usando qualquer uma dessas cinco dimensões: esperas, SQL, hosts, usuários e bancos de dados. Essas dimensões são subcategorias doDBLoadmétrica. Você pode usá-los como fatia por categorias para representar características diferentes da carga do banco de dados. Para obter uma descrição detalhada de como calculamos a carga do banco de dados, consulte [Carregar banco de dados](#) na documentação do Amazon RDS.

A ilustração da tela a seguir mostra a ferramenta Performance Insights.



Dimensões

- Aguarde eventossão condições pelas quais uma sessão do banco de dados espera que um recurso ou outra operação seja concluída para continuar seu processamento. Se você executar uma instrução SQL, como `SELECT * FROM big_table` se essa tabela for muito maior do que o buffer pool alocado do InnoDB, sua sessão provavelmente aguardará `wait/io/file/innodb/innodb_data_file` eventos de espera, que são causados por operações físicas de E/S no arquivo de dados. Os eventos de espera são uma dimensão importante para o monitoramento do banco de dados, pois indicam possíveis gargalos de desempenho. Os eventos de espera indicam os recursos e as operações que as instruções SQL que você está executando nas sessões passam mais tempo esperando. Por exemplo, o `wait/synch/mutex/innodb/trx_sys_mutex` evento ocorre quando há alta atividade no banco de dados com um grande número de transações, e o `wait/synch/mutex/innodb/buf_pool_mutex` evento ocorre quando um thread adquire um bloqueio no buffer pool do InnoDB para acessar uma página na memória. Para obter informações sobre todos os eventos de espera do MySQL e do MariaDB, consulte [Tabelas de resumo do evento Wait](#) na documentação do MySQL. Para entender como

interpretar os nomes dos instrumentos, consulte [Convenções de nomenclatura de instrumentos do Esquema de Desempenho](#) na documentação do MySQL.

- SQL mostra quais instruções SQL estão contribuindo mais para a carga total do banco de dados. O Dimensões superiores tabela, que está localizada sob o Carregar banco de dados O gráfico no Amazon RDS Performance Insights é interativo. Você pode obter uma lista detalhada dos eventos de espera associados à instrução SQL clicando na barra na Carga por espera (AAS) coluna. Quando você seleciona uma instrução SQL na lista, o Performance Insights exibe os eventos de espera associados na Carregar banco de dados gráfico e o texto da instrução SQL no Texto SQL seção. As estatísticas do SQL são exibidas no lado direito do Dimensões superiores mesa.
- anfitriões mostra os nomes dos anfitriões dos clientes conectados. Essa dimensão ajuda a identificar quais hosts do cliente estão enviando a maior parte da carga para o banco de dados.
- Usuários agrupe a carga do banco de dados por usuários que estão conectados ao banco de dados.
- bancos de dados agrupe a carga do banco de dados pelo nome do banco de dados ao qual o cliente está conectado.

Métricas de contador

As métricas contadoras são métricas cumulativas cujos valores só podem aumentar ou redefinir para zero quando a instância de banco de dados é reiniciada. O valor de uma métrica contadora não pode ser reduzido ao valor anterior. Essas métricas representam um contador único e monotonicamente crescente.

- [Contadores nativos](#) são métricas definidas pelo mecanismo de banco de dados e não pelo Amazon RDS. Por exemplo:
 - `SQL.Innodb_rows_inserted` representa o número de linhas inseridas nas tabelas do InnoDB.
 - `SQL.Select_scan` representa o número de junções que concluíram uma verificação completa da primeira tabela.
 - `Cache.Innodb_buffer_pool_reads` representa o número de leituras lógicas que o mecanismo InnoDB não conseguiu recuperar do buffer pool e precisou ler diretamente do disco.
 - `Cache.Innodb_buffer_pool_read_requests` representa o número de solicitações de leitura lógica.

Para obter definições de todas as métricas nativas, consulte [Variáveis de status do servidor](#) na documentação do MySQL.

- [Contadores não nativos](#) são definidos pelo Amazon RDS. Você pode obter essas métricas usando uma consulta específica ou derivá-las usando duas ou mais métricas nativas nos cálculos. As métricas de contador não nativas podem representar latências, índices ou taxas de acerto. Por exemplo:

- `Cache.innoDB_buffer_pool_hits` representa o número de operações de leitura que o InnoDB poderia recuperar do buffer pool sem utilizar o disco. Ele é calculado a partir das métricas nativas do contador da seguinte forma:

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

- `IO.innoDB_datafile_writes_to_disk` representa o número de operações de gravação de arquivos de dados do InnoDB no disco. Ele captura somente operações em arquivos de dados, não operações de gravação dupla ou de regravação em log. É calculado da seguinte forma:

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

Você pode visualizar as métricas da instância de banco de dados diretamente no painel do Performance Insights. Escolha **Gerenciar métricas**, escolha **o métricas do banco de dados** guia e, em seguida, selecione as métricas de interesse, conforme mostrado na ilustração a seguir.

Select metrics shown on the graph

OS metrics (0)

Database metrics (6)

Clear all selections

▼ SQL

☐ Com_analyze

☐ Com_select

☐ Innodb_rows_deleted

☐ Innodb_rows_read

☒ Queries

☐ Select_full_range_join

☐ Select_range_check

☐ Slow_queries

☐ Sort_range

☒ Sort_scan

☐ Com_optimize

☐ Innodb_rows_inserted

☐ Innodb_rows_updated

☐ Questions

☐ Select_full_join

☐ Select_range

☒ Select_scan

☐ Sort_merge_passes

☐ Sort_rows

☐ innodb_rows_changed

▼ Locks

☐ Innodb_row_lock_time

☐ innodb_deadlocks

☐ Table_locks_immediate

☒ innodb_row_lock_waits

☐ innodb_lock_timeouts

☐ Table_locks_waited

▼ Users

☒ Connections

☐ Aborted_connects

☐ Threads_created

☐ Aborted_clients

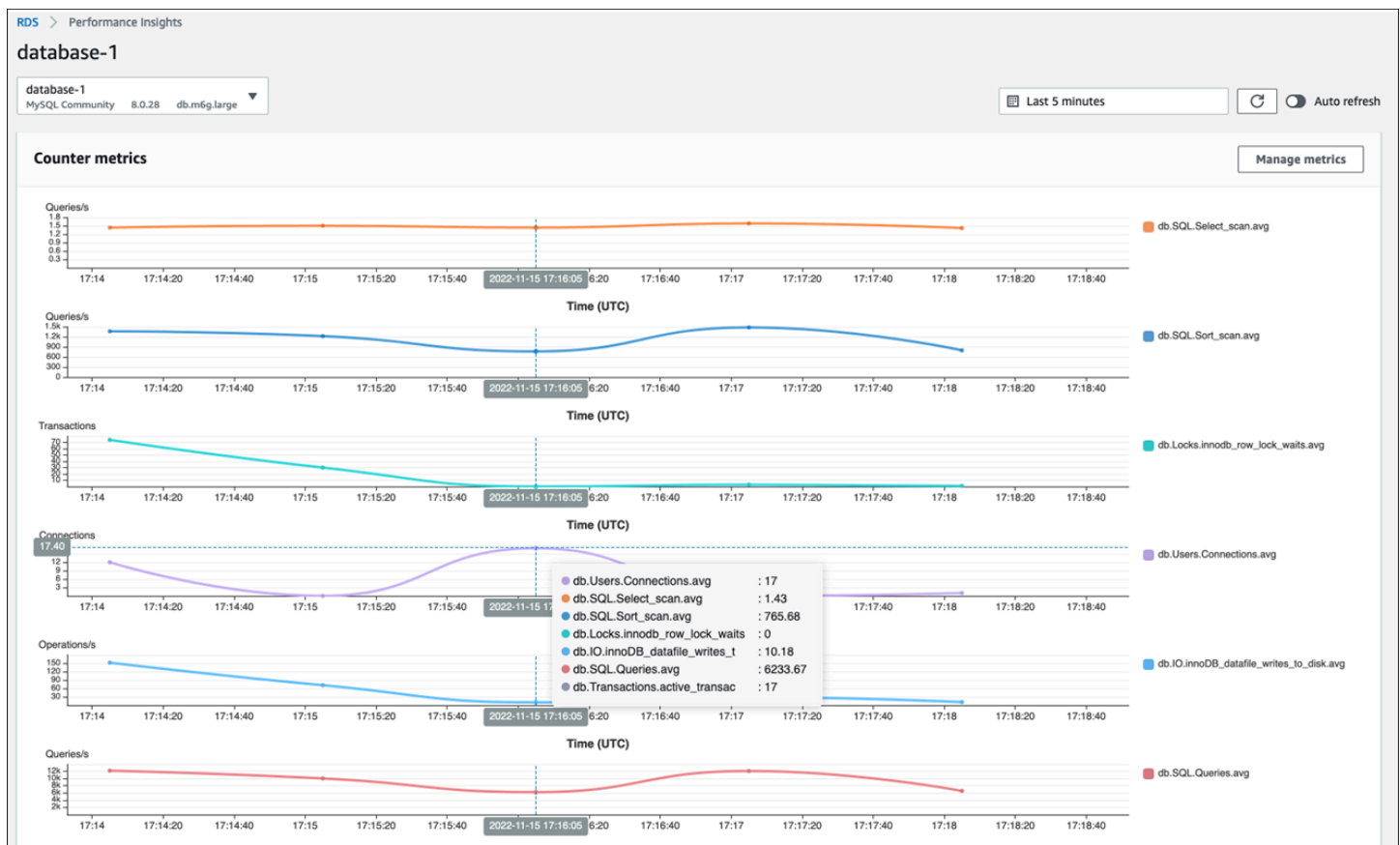
☐ Threads_running

☐ Threads_connected

Cancel

Update graph

Escolha oGráfico de atualizaçãobotão para exibir as métricas selecionadas, conforme mostrado na ilustração a seguir.



Estatísticas SQL

O Performance Insights reúne métricas relacionadas ao desempenho sobre consultas SQL para cada segundo em que uma consulta está sendo executada e para cada chamada SQL. Em geral, o Performance Insights coleta [Estatísticas do SQL](#) nos níveis de declaração e resumo. No entanto, para instâncias de banco de dados MariaDB e MySQL, as estatísticas são coletadas somente no nível do resumo.

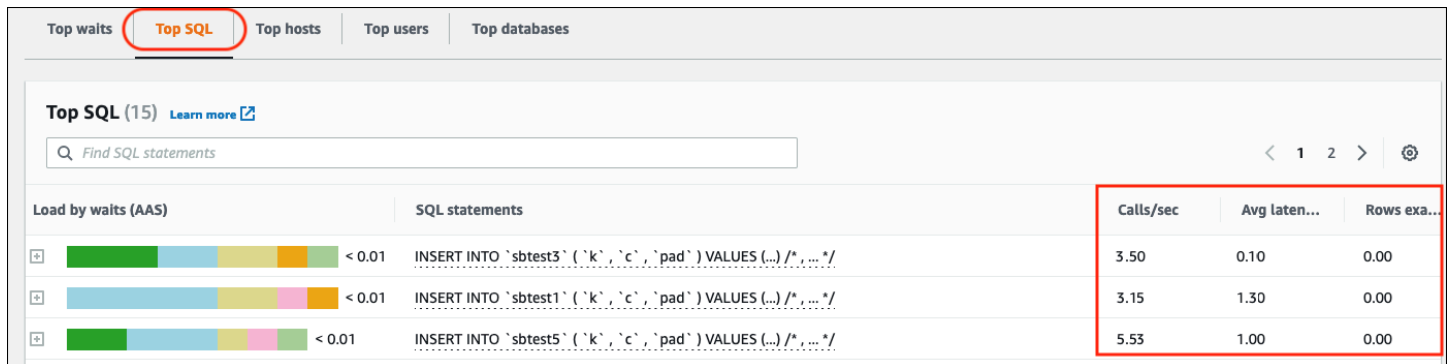
- As estatísticas de resumo são uma métrica composta de todas as consultas que têm o mesmo padrão, mas que eventualmente têm valores literais diferentes. O resumo substitui valores literais específicos por uma variável; por exemplo:

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

- Existem métricas que representam estatísticas por segundo para cada instrução SQL digerida. Por exemplo, `sql_tokenized.stats.count_star_per_sec` representa chamadas por segundo (ou seja, quantas vezes por segundo a instrução SQL foi executada).

- O Performance Insights também inclui métricas que fornecem por chamada estatísticas para uma instrução SQL. Por exemplo, `sql_tokenized.stats.sum_timer_wait_per_call` mostra a latência média da instrução SQL por chamada, em milissegundos.

As estatísticas do SQL estão disponíveis no painel do Performance Insights, no Melhor SQL Laba do Dimensões superiores mesa.



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 instâncias de banco de dados

Amazon CloudWatch também contém métricas que o Amazon RDS publica automaticamente. As métricas que residem no AWS/RDS namespaces são métricas em nível de instância, que se refere à instância (serviço) do Amazon RDS (ou seja, ao ambiente de banco de dados isolado em execução na nuvem) em vez da instância de banco de dados no sentido estrito do `mysqld` processo. Portanto, a maioria desses [métricas padrão](#) se enquadram na categoria de métricas do sistema operacional, na definição estrita do termo. Os exemplos incluem: `CPUUtilization`, `WriteIOPS`, `SwapUsage` e outros. No entanto, existem algumas métricas de instância de banco de dados aplicáveis ao MariaDB e ao MySQL:

- `BinLogDiskUsage`— A quantidade de espaço em disco ocupado pelos registros binários.
- `DatabaseConnections`— O número de conexões de rede do cliente com a instância de banco de dados.
- `ReplicaLag`— A quantidade de tempo que uma instância de banco de dados de réplica de leitura fica atrasada em relação à instância de banco de dados de origem.

Publicando métricas do Performance Insights emCloudWatch

O Amazon RDS Performance Insights monitora a maioria das métricas e dimensões da instância de banco de dados e as disponibiliza por meio do painel Performance Insights no [AWSConsole de gerenciamento](#). Esse painel é adequado para solução de problemas de banco de dados e análise da causa raiz. No entanto, não é possível criar alarmes no Performance Insights para métricas relacionadas ao desempenho. Para criar alarmes com base nas métricas do Performance Insights, você precisa mover essas métricas paraCloudWatch. Ter as métricas emCloudWatchtambém oferece acesso a recursos avançados de monitoramento, como [CloudWatchdetecção de anomalias](#), [matemática métrica](#), e [estatísticas](#), e você pode exportar as métricas para ferramentas de monitoramento externas, como Prometheus e Grafana.

As métricas do Performance Insights não são publicadas automaticamente noCloudWatch(exceto para o [métrica DBLoad](#)). Para publicar as métricas da instância de banco de dados do Performance Insights paraCloudWatch, você pode usar o [API Performance Insights](#) para recuperar métricas e o [CloudWatchAPI](#) para publicar métricas emCloudWatch. Para automatizar o processo, você pode criar uma função Lambda e agendá-la na AmazonEventBridgepara ser executado em períodos de tempo especificados, por exemplo, a cada dois minutos. Você pode especificar em quais métricas do Performance Insights você deseja publicarCloudWatch. A função Lambda obtém essas métricas de todas as instâncias do Amazon RDS que têm o Performance Insights ativado e salva as métricas emCloudWatch. Para obter mais informações sobre esse processo, consulte a postagem do blog sobre [fornecendo métricas de contador do Performance Insights paraCloudWatch](#).

Monitoramento do SO

Uma instância de banco de dados no Amazon RDS para MySQL ou MariaDB é executada no sistema operacional Linux, que usa recursos subjacentes do sistema: CPU, memória, rede e armazenamento.

```
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)
```

O desempenho geral do banco de dados e do sistema operacional subjacente depende fortemente da utilização dos recursos do sistema. Por exemplo, a CPU é o componente chave para o desempenho do sistema, pois executa as instruções do software do banco de dados e gerencia outros recursos do sistema. Se a CPU for superutilizada (ou seja, se a carga exigir mais energia da CPU do que a provisionada para sua instância de banco de dados), esse problema afetará o desempenho e a estabilidade do seu banco de dados e, conseqüentemente, do seu aplicativo.

O mecanismo de banco de dados aloca e libera memória dinamicamente. Quando não há memória suficiente na RAM para fazer o trabalho atual, o sistema grava páginas de memória na memória de troca, que reside no disco. Como o disco é muito mais lento do que a memória, mesmo que o disco seja baseado na tecnologia SSD NVMe, a alocação excessiva de memória leva à degradação do desempenho. A alta utilização da memória causa maior latência das respostas do banco de dados, porque o tamanho de um arquivo de paginação aumenta para suportar memória adicional. Se a alocação de memória for tão alta que esgote os espaços de memória RAM e de troca, o serviço de banco de dados poderá ficar indisponível e os usuários poderão observar erros como [ERROR] mysqld: Out of memory (Needed xyz bytes).

Os sistemas de gerenciamento de banco de dados MySQL e MariaDB utilizam o subsistema de armazenamento, que consiste em discos que armazenam [estruturas em disco](#) como tabelas, índices, registros binários, redo logs, registros de desfazer e arquivos de buffer de gravação dupla. Portanto,

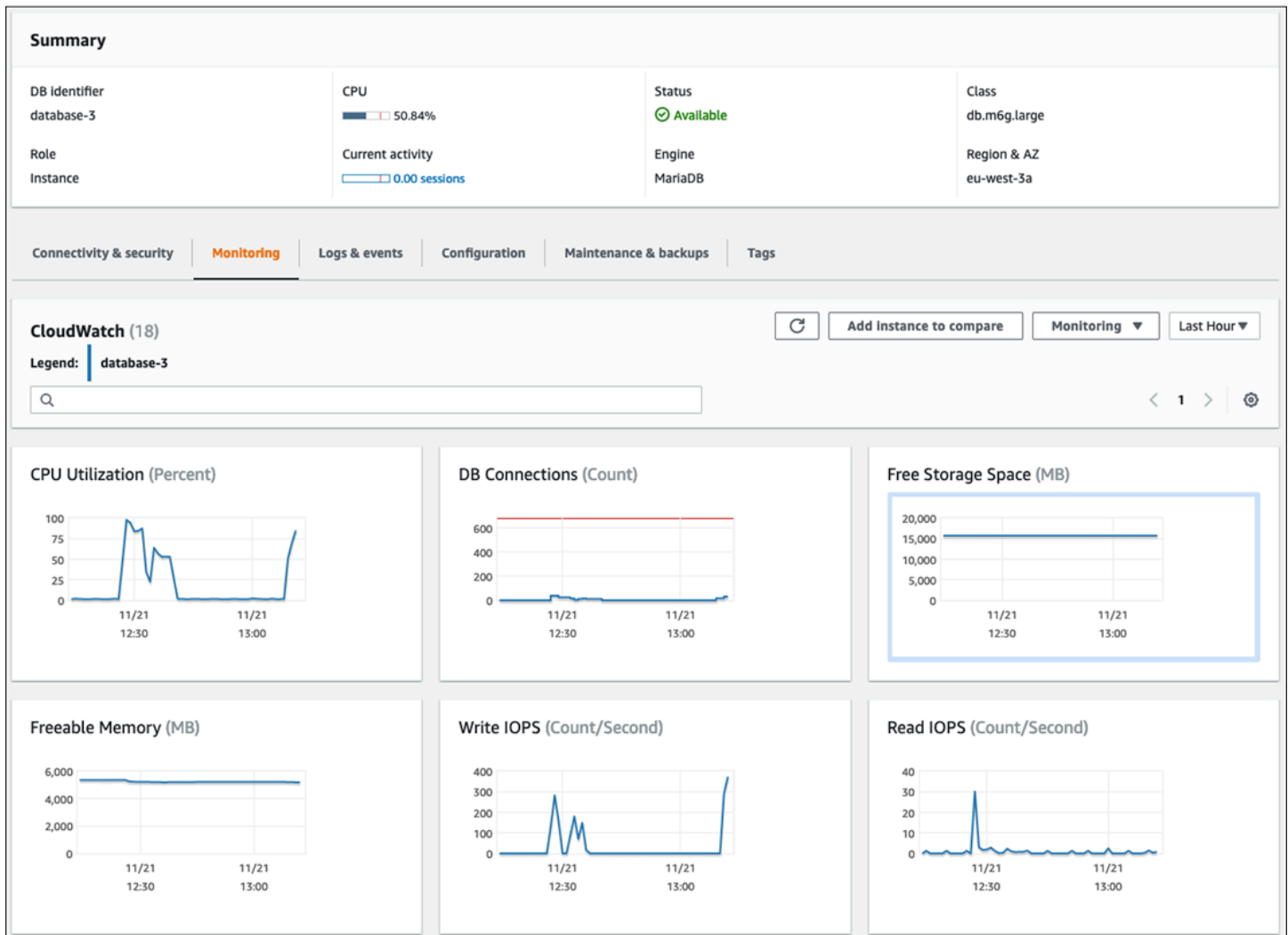
o banco de dados, ao contrário de outros tipos de software, deve realizar muitas atividades no disco. Para a operação ideal do seu banco de dados, é importante monitorar e ajustar a utilização de E/S do disco e a alocação do espaço em disco. O desempenho do banco de dados pode ser afetado quando o banco de dados atinge as limitações de IOPS ou taxa de transferência máxima suportada pelo disco. Por exemplo, surtos de acesso aleatório causados por uma verificação de índice podem causar um grande número de operações de I/O por segundo, o que eventualmente pode atingir as limitações do armazenamento subjacente. Os escaneamentos completos da tabela podem não atingir o limite de IOPS, mas podem causar uma alta taxa de transferência, medida em megabytes por segundo. É fundamental monitorar e gerar alertas sobre a alocação de espaço em disco, pois erros como `OS error code 28: No space left on device` pode causar indisponibilidade e corrupção do banco de dados.

O Amazon RDS fornece métricas em tempo real para o sistema operacional em que sua instância de banco de dados é executada. O Amazon RDS publica automaticamente um conjunto de métricas do sistema operacional para CloudWatch. Essas métricas estão disponíveis para exibição e análise no console do Amazon RDS e no CloudWatch painéis, e você pode definir alarmes nas métricas selecionadas em CloudWatch. Os exemplos incluem:

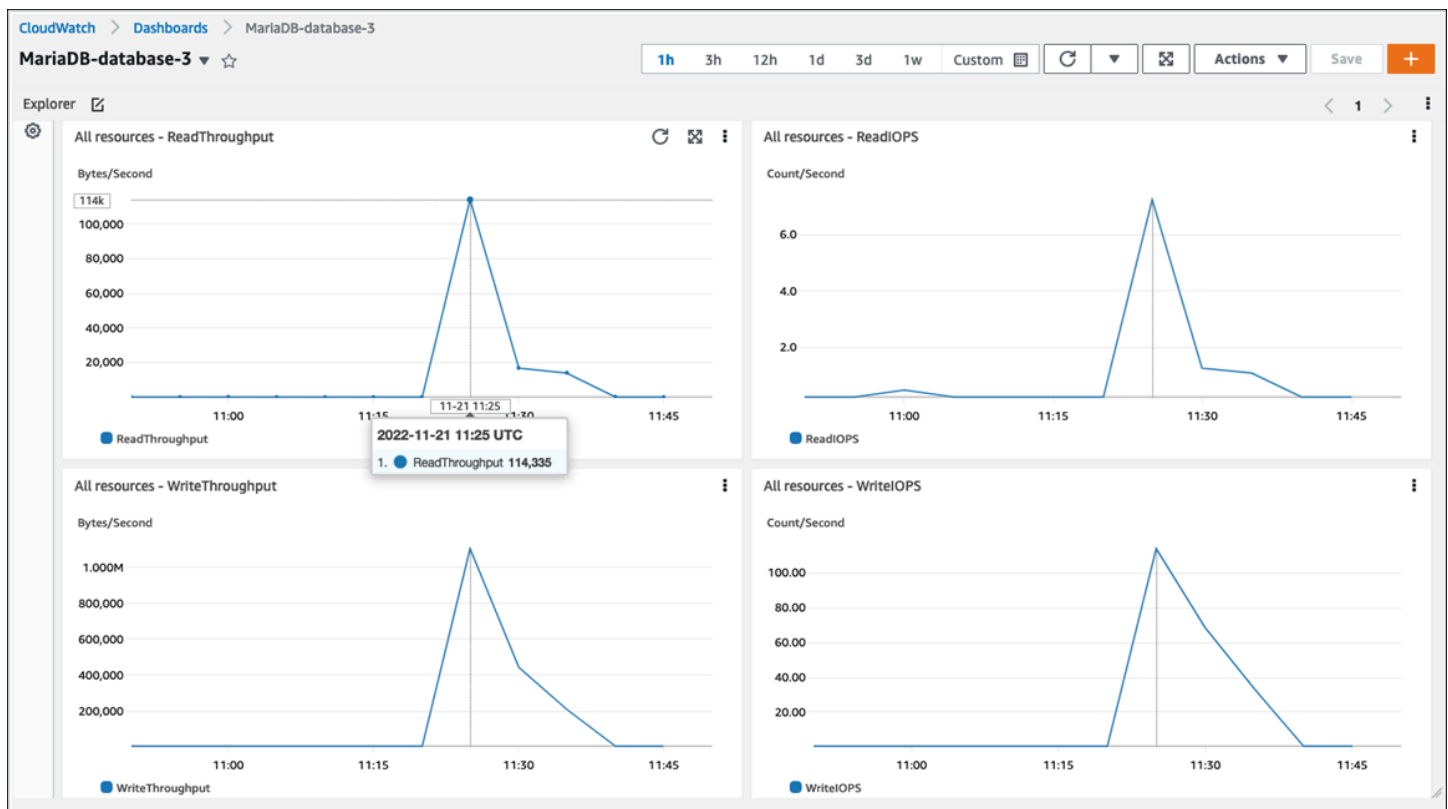
- `CPUUtilization`— A porcentagem de utilização da CPU.
- `BinLogDiskUsage`— A quantidade de espaço em disco que é ocupada pelos registros binários.
- `FreeableMemory`— A quantidade de memória de acesso aleatório disponível. Isso representa o valor do `MemAvailable` campo de `/proc/meminfo`.
- `ReadIOPS`— O número médio de operações de E/S de leitura de disco por segundo.
- `WriteThroughput`— O número médio de bytes gravados em disco por segundo para armazenamento local.
- `NetworkTransmitThroughput`— O tráfego de rede de saída no nó de banco de dados, que combina o tráfego do banco de dados e o tráfego do Amazon RDS usado para monitoramento e replicação.

Para obter uma referência completa de todas as métricas publicadas pelo Amazon RDS, CloudWatch, veja [Amazon CloudWatch métricas para o Amazon RDS](#) na documentação do Amazon RDS.

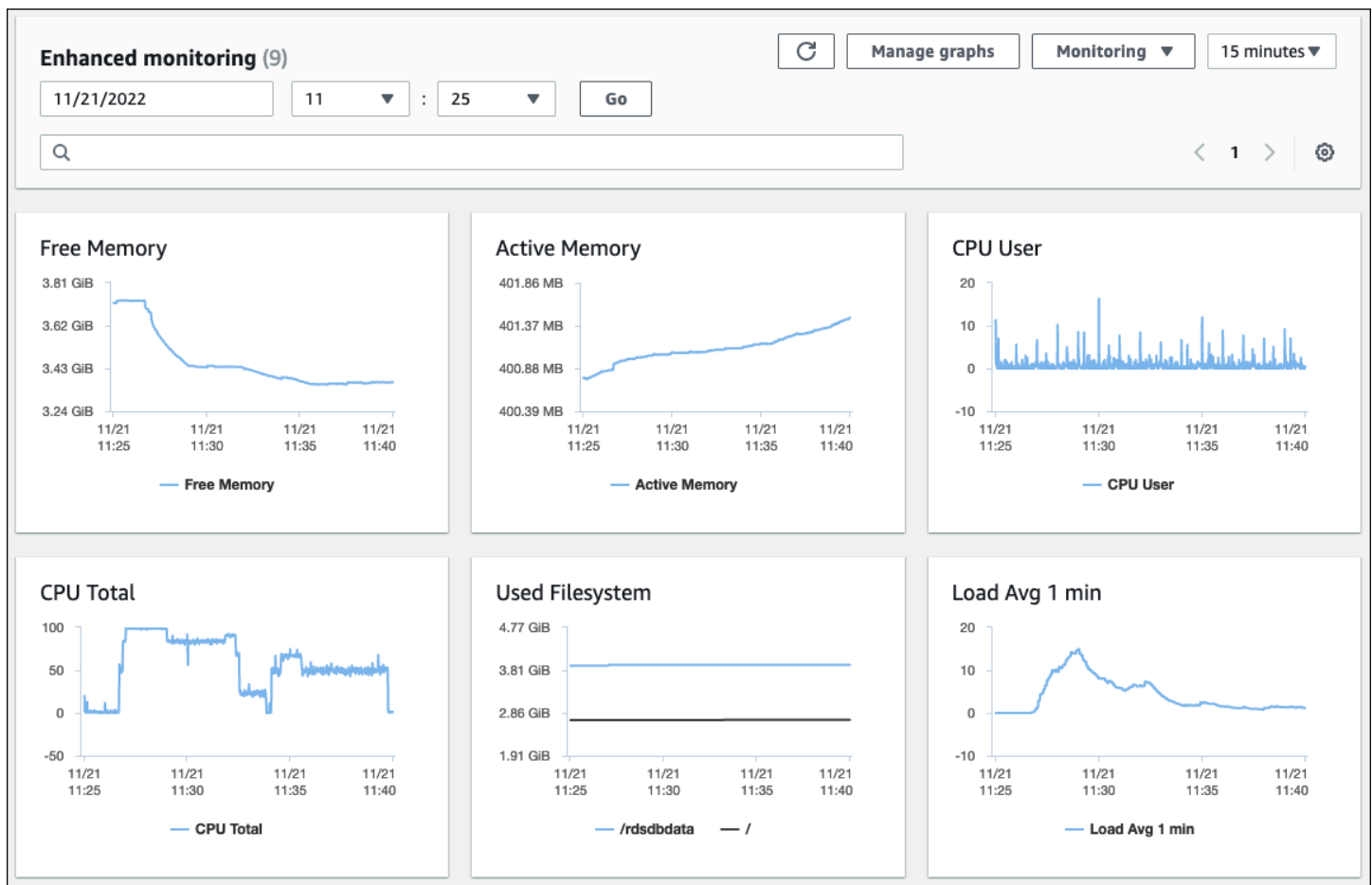
O gráfico a seguir mostra exemplos de CloudWatch métricas do Amazon RDS que são exibidas no console do Amazon RDS.



O gráfico a seguir mostra métricas semelhantes exibidas na CloudWatch painel de controle.



O outro conjunto de métricas do sistema operacional é coletado por [Monitoramento aprimorado](#) para o Amazon RDS. Essa ferramenta oferece uma visibilidade mais profunda da integridade de suas instâncias de banco de dados Amazon RDS para MariaDB e Amazon RDS para MySQL, fornecendo métricas do sistema em tempo real e informações do processo do sistema operacional. Quando você [ativar o monitoramento aprimorado](#) em sua instância de banco de dados e define a granularidade desejada, a ferramenta coleta as métricas do sistema operacional e as informações do processo, que você pode exibir e analisar no [Console Amazon RDS](#), conforme mostrado na tela a seguir.



Algumas das principais métricas fornecidas pelo Enhanced Monitoring são:

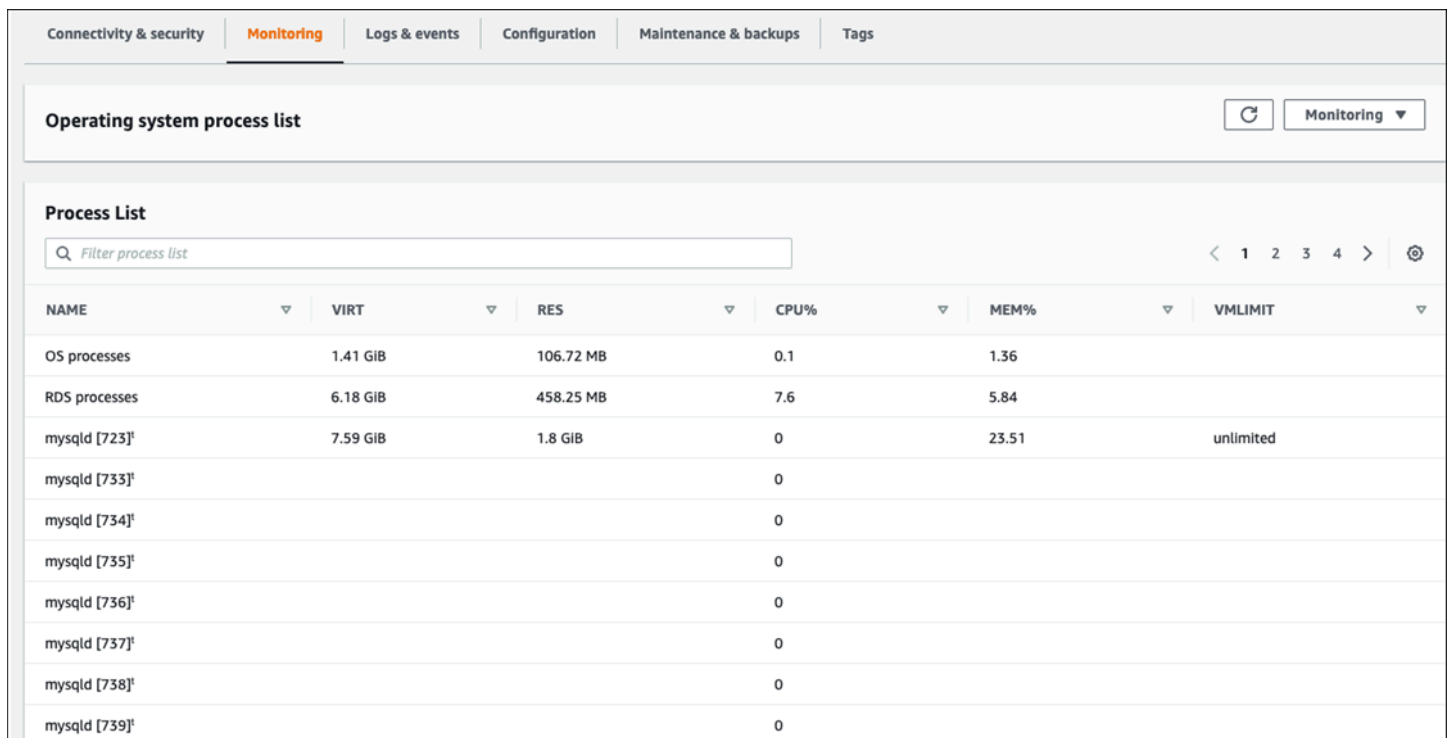
- `cpuUtilization.total`— A porcentagem total da CPU em uso.
- `cpuUtilization.user`— A porcentagem de CPU em uso pelos programas do usuário.
- `memory.active`— A quantidade de memória atribuída, em kilobytes.
- `memory.cached`— A quantidade de memória usada para armazenar em cache a E/S baseada no sistema de arquivos.
- `loadAverageMinute.one`— O número de processos que solicitaram tempo de CPU durante o último minuto.

Para obter uma lista completa de métricas, consulte [Métricas do sistema operacional no monitoramento aprimorado](#) na documentação do Amazon RDS.

No console do Amazon RDS, a lista de processos do sistema operacional fornece detalhes de cada processo em execução na sua instância de banco de dados. A lista está organizada em três seções:

- **Processos do sistema operacional**— Esta seção representa um resumo agregado de todos os processos do kernel e do sistema. Esses processos geralmente têm um impacto mínimo no desempenho do banco de dados.
- **Processos RDS**— Esta seção representa um resumo dos processos do AWS que são necessários para dar suporte a uma instância de banco de dados Amazon RDS. Por exemplo, inclui o agente de gerenciamento do Amazon RDS, processos de monitoramento e diagnóstico e processos similares.
- **Processos infantis do RDS**— Esta seção representa um resumo dos processos do Amazon RDS que oferecem suporte à instância de banco de dados – neste caso, o `mysqld` processo e seus filhos. Os filhos do `mysqld` aparecem aninhados abaixo do `mysqld` processo.

A ilustração da tela a seguir mostra a lista de processos do sistema operacional no console do Amazon RDS.

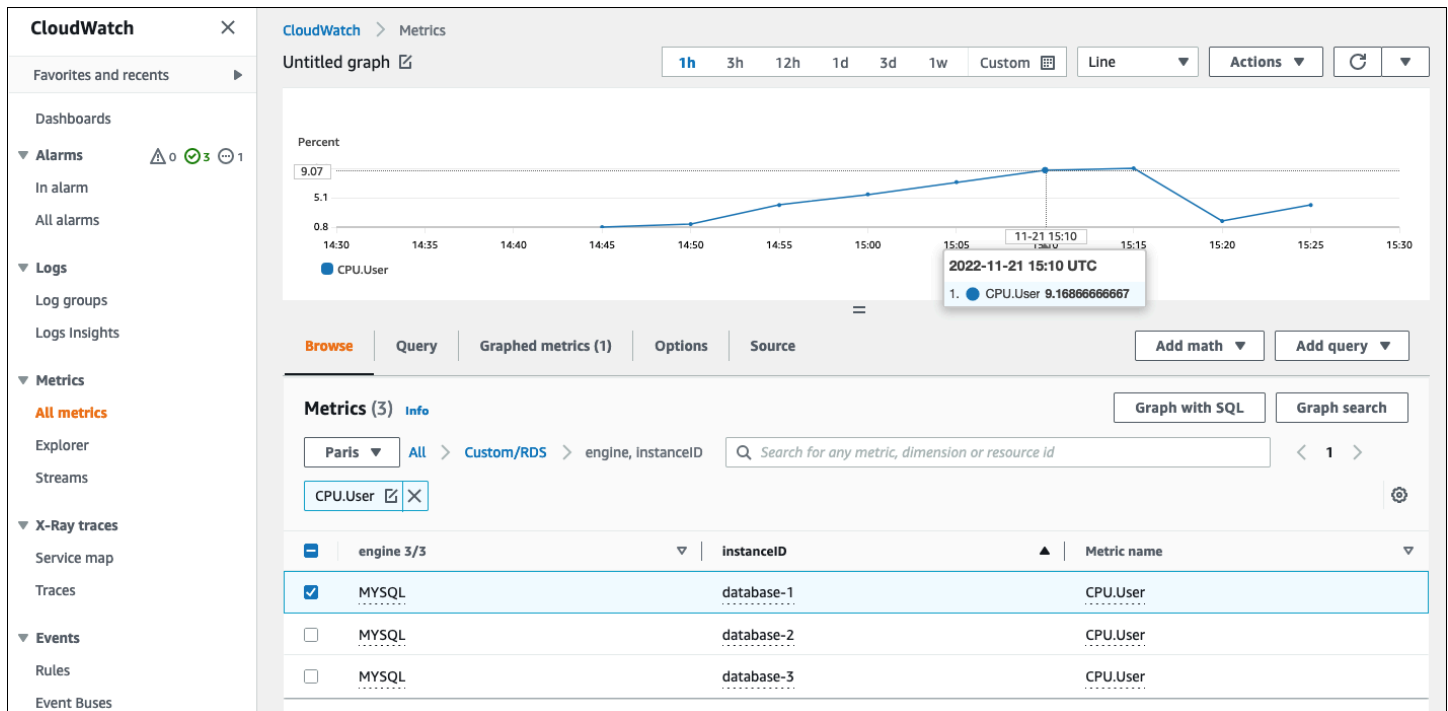


NAME	VIRT	RES	CPU%	MEM%	VMLIMIT
OS processes	1.41 GiB	106.72 MB	0.1	1.36	
RDS processes	6.18 GiB	458.25 MB	7.6	5.84	
mysqld [723]	7.59 GiB	1.8 GiB	0	23.51	unlimited
mysqld [733]			0		
mysqld [734]			0		
mysqld [735]			0		
mysqld [736]			0		
mysqld [737]			0		
mysqld [738]			0		
mysqld [739]			0		

O Amazon RDS fornece as métricas do monitoramento aprimorado em seu CloudWatch Conta de registros. Os dados de monitoramento que são exibidos no console do Amazon RDS são recuperados de CloudWatch Registros. Você também pode [recuperar as métricas de uma instância de banco de dados como um fluxo de log](#) desde CloudWatch Registros. Essas métricas são armazenadas no formato JSON. Você pode consumir a saída JSON do Enhanced Monitoring do CloudWatch Registra um sistema de monitoramento de sua escolha.

Para exibir gráficos no CloudWatch painel e criar alarmes que iniciariam uma ação se uma métrica violasse o limite definido, você deve criar filtros métricos no CloudWatch desde CloudWatch Registros. Para obter instruções detalhadas, consulte o [Artigo do AWS Re:posts](#) sobre como filtrar o monitoramento aprimorado CloudWatch Registros para gerar métricas personalizadas automatizadas para o Amazon RDS.

O exemplo a seguir ilustra a métrica personalizada `CPU.User` na `Custom/RDS` namespace. Essa métrica personalizada é criada filtrando `cpuUtilization.user` Métrica de monitoramento aprimorada de CloudWatch Registros.



Quando a métrica está disponível no CloudWatch repositório, você pode exibi-la e analisá-la em CloudWatch painéis, aplique mais operações matemáticas e de consulta e defina um alarme para monitorar essa métrica específica e gerar alertas se os valores observados não estiverem de acordo com as condições de alarme definidas.

Eventos, registros e trilhas de auditoria

Monitoramento [métricas da instância de banco de dados](#) e [Métricas do sistema operacional](#), analisar as tendências e comparar métricas com valores básicos e gerar alertas quando os valores ultrapassam os limites definidos são todas práticas necessárias e recomendadas que ajudam você a alcançar e manter a confiabilidade, disponibilidade, desempenho e segurança de suas instâncias de banco de dados Amazon RDS. No entanto, uma solução completa também deve monitorar eventos de banco de dados, arquivos de log e trilhas de auditoria dos bancos de dados MySQL e MariaDB.

Seções

- [Eventos do Amazon RDS](#)
- [Registros do banco](#)
- [Trilhas de auditoria](#)

Eventos do Amazon RDS

Um **Evento RDS** indica uma mudança no ambiente do Amazon RDS. Por exemplo, quando o status da instância de banco de dados muda de **Começando** para **Disponível**, o Amazon RDS gera o evento **RDS-EVENT-0088 The DB instance has been started**. O Amazon RDS entrega eventos para a **Amazon EventBridge** quase em tempo real. Você pode acessar eventos por meio do console do Amazon RDS, o **AWS CLI** ou o **AWS SDK** com o comando [descrever eventos](#), ou a operação da API Amazon RDS [DescribeEvents](#). A ilustração da tela a seguir mostra eventos e registros exibidos no console do 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	

O Amazon RDS emite diferentes tipos de eventos, incluindo eventos de instância de banco de dados, eventos de grupo de parâmetros de banco de dados, eventos de grupo de segurança de banco de dados, eventos de snapshot de banco de dados, eventos de proxy do RDS e eventos de implantação azul/verde. As informações incluem:

- Nome e tipo de fonte; por exemplo: "SourceIdentifier": "database-1", "SourceType": "db-instance"
- Data e hora do evento; por exemplo: "Date": "2022-12-01T09:20:28.595000+00:00"
- Mensagem associada ao evento; por exemplo: "Message": "Finished updating DB parameter group"
- Categoria do evento; por exemplo: "EventCategories": ["configuration change"]

Para obter uma referência completa, consulte [Categorias de eventos e mensagens de eventos do Amazon RDS](#) na documentação do Amazon RDS.

Recomendamos que você monitore os eventos do Amazon RDS, pois esses eventos indicam mudanças de status na disponibilidade de instâncias de banco de dados, alterações de configuração, alterações no status da réplica de leitura, eventos de backup e recuperação, ações de failover, eventos de falha, modificações nos grupos de segurança e muitas outras notificações. Por exemplo, se você configurou uma instância de banco de dados de réplica de leitura para fornecer desempenho e durabilidade aprimorados ao seu banco de dados, recomendamos que você monitore os eventos do Amazon RDS para obter a categoria de evento associada a instâncias de banco de dados. Isso ocorre porque eventos como RDS-EVENT-0057 Replication on the read replica was terminated indique que sua réplica de leitura não está mais sincronizada com a instância de banco de dados primária. Uma notificação à equipe responsável de que tal evento aconteceu pode ajudar a mitigar o problema em tempo hábil. Além dos serviços adicionais da AWS, como AWS Lambda, o Amazon Simple Queue Service (Amazon SQS) e o Amazon Simple Notification Service (Amazon SNS) podem ajudar você a automatizar respostas a eventos do sistema, como problemas de disponibilidade do banco de dados ou alterações de recursos.

No console do Amazon RDS, você pode recuperar eventos das últimas 24 horas. Se você usar o AWS CLI ou a API do Amazon RDS para visualizar eventos, você pode recuperar eventos dos últimos 14 dias usando o seguinte comando da seguinte forma.

```
$ 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"
    }
  ]
}

```

Se você quiser armazenar eventos de longo prazo, até o período de expiração especificado ou permanentemente, você pode usar [CloudWatch Registros](#) para registrar as informações sobre os eventos que foram gerados pelo Amazon RDS. Para implementar essa solução, você pode usar um tópico do Amazon SNS para receber notificações de eventos do Amazon RDS e, em seguida, chamar uma função do Lambda para registrar o evento `CloudWatchRegistros`.

1. Crie uma função Lambda que será chamada no evento e registre as informações do evento em `CloudWatchRegistros`. `CloudWatch Logs` é integrado ao Lambda e fornece uma maneira conveniente de registrar informações de eventos, usando o `print` para `stdout`.
2. Crie um tópico do SNS com uma assinatura de uma função Lambda (conjunto de protocolo para Lambda) e defina o ponto final para o Amazon Resource Name (ARN) da função Lambda que você criou na etapa anterior.
3. Configure seu tópico do SNS para receber notificações de eventos do Amazon RDS. Para obter instruções detalhadas, consulte o [AWSRe:post do artigo](#) sobre como fazer com que seu tópico do Amazon SNS receba notificações do Amazon RDS.
4. No console do Amazon RDS, crie uma nova assinatura de evento. Conjunto de protocolo para o ARN e, em seguida, selecione o tópico do SNS que você criou anteriormente. Conjunto de tipo de

fonteeCategorias de eventos a serem incluídasde acordo com suas necessidades. Para obter mais informações, consulte[Inscrever-se na notificação de eventos do Amazon RDS](#)na documentação do Amazon RDS.

Registros do banco

Os bancos de dados MySQL e MariaDB geram registros que você pode acessar para auditoria e solução de problemas. Esses registros são:

- [Auditoria](#)— A trilha de auditoria é um conjunto de registros que registram a atividade do servidor. Para cada sessão do cliente, ele registra quem se conectou ao servidor (nome de usuário e host), quais consultas foram executadas, quais tabelas foram acessadas e quais variáveis do servidor foram alteradas.
- [Erro](#)— Esse log contém o do servidor (mysqld) tempos de inicialização e desligamento e mensagens de diagnóstico, como erros, avisos e notas, que ocorrem durante a inicialização e o desligamento do servidor e enquanto o servidor está em execução.
- [Geral](#)— Este registro registra a atividade de mysqld, incluindo a atividade de conexão e desconexão de cada cliente e as consultas SQL recebidas dos clientes. O registro geral de consultas pode ser muito útil quando você suspeita de um erro e deseja saber exatamente para o que o cliente enviou.mysqld.
- [Consulta lenta](#)— Esse log fornece um registro das consultas SQL que demoraram muito para serem executadas.

Como melhor prática, você deve[publicar registros de banco de dados do Amazon RDS para a AmazonCloudWatchRegistros](#). ComCloudWatchRegistros, você pode realizar análises em tempo real dos dados de registro, armazenar os dados em um armazenamento altamente durável e gerenciar os dados com oCloudWatchAgente de registros. Você pode[acesse e monitore seus registros de banco de dados](#)do console Amazon RDS. Você também pode usarCloudWatchLogs Insights para pesquisar e analisar interativamente seus dados de registro noCloudWatchRegistros. O exemplo a seguir ilustra uma consulta no registro de auditoria que verifica quantas vezesCONNECTos eventos aparecem no registro, quem se conectou e de qual cliente (endereço IP) eles se conectaram. O trecho do registro de auditoria pode ter a seguinte aparência:

```
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
```

O exemplo de consulta do Log Insights mostra que `rdsadmin` conectou ao banco de dados a partir de `localhost` a cada 5 minutos, totalizando 22 vezes, conforme mostrado na ilustração a seguir.

Esses resultados indicam que a atividade se originou de processos internos do Amazon RDS, como o próprio sistema de monitoramento.

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 X

```

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 ⓘ Hide histogram

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

Os eventos de registro geralmente incluem mensagens importantes que você deseja contar, como avisos ou erros sobre operações associadas às instâncias de banco de dados MySQL e

MariaDB. Por exemplo, se uma operação falhar, um erro pode ocorrer e ser registrado no arquivo de registro de erros da seguinte forma: `ERROR 1114 (HY000): The table zip_codes is full`. Talvez você queira monitorar essas entradas para entender a tendência de seus erros. Você pode [criar personalizado CloudWatch métricas dos registros do Amazon RDS usando filtros](#) para habilitar o monitoramento automático dos registros do banco de dados do Amazon RDS para monitorar um registro específico para padrões específicos e gerar um alarme se houver violações do comportamento esperado. [Por exemplo](#), crie um filtro métrico para o grupo de registros `/aws/rds/instance/database-1/error` que monitoraria o registro de erros e procuraria o [padrão específico](#), como `ERROR`. Defina o Padrão de filtro para `ERROR` e o Valor métrico para `1`. O filtro detectará cada registro de registro que tenha a palavra-chave `ERROR` e incrementará a contagem em 1 para cada evento de log que contenha “ERROR”. Depois de criar o filtro, você pode definir um alarme para notificá-lo caso sejam detectados erros no log de erros do MySQL ou do MariaDB.

Para saber mais sobre como monitorar o log de consultas lentas e o log de erros, criando um [CloudWatch painel](#) e usando [CloudWatch Logs Insights](#), veja a postagem do blog [Criando uma Amazon CloudWatch painel para monitorar o Amazon RDS e o Amazon Aurora MySQL](#).

Trilhas de auditoria

A trilha de auditoria (ou registro de auditoria) fornece um registro cronológico e relevante para a segurança dos eventos em sua conta da AWS. Inclui eventos para o Amazon RDS, que fornecem evidências documentais da sequência de atividades que afetaram seu banco de dados ou seu ambiente de nuvem. No Amazon RDS para MySQL ou MariaDB, o uso da trilha de auditoria envolve:

- Monitoramento do registro de auditoria da instância de banco de dados
- Monitoramento de chamadas de API do Amazon RDS em AWS CloudTrail

Para uma instância de banco de dados Amazon RDS, os objetivos da auditoria geralmente incluem:

- Permitindo a responsabilidade pelo seguinte:
 - Modificações realizadas no parâmetro ou na configuração de segurança
 - Ações executadas em um esquema, tabela ou linha do banco de dados, ou ações que afetam conteúdo específico
- Detecção e investigação de intrusões
- Detecção e investigação de atividades suspeitas

- Detecção de problemas de autorização; por exemplo, para identificar abusos de direitos de acesso por usuários regulares ou privilegiados

A trilha de auditoria do banco de dados tenta responder a essas perguntas típicas: Quem visualizou ou modificou dados confidenciais em seu banco de dados? Quando isso aconteceu? De onde um usuário específico acessou os dados? Usuários privilegiados abusaram de seus direitos de acesso ilimitado?

Tanto o MySQL quanto o MariaDB implementam o recurso de trilha de auditoria da instância de banco de dados usando o MariaDB Audit Plugin. Esse plug-in registra a atividade do banco de dados, como usuários fazendo login no banco de dados e consultas em execução no banco de dados. O registro da atividade do banco de dados é armazenado em um arquivo de log. Para acessar o log de auditoria, a instância de banco de dados deve usar um grupo de opções personalizado com a opção `MARIADB_AUDIT_PLUGIN`. Para obter mais informações, consulte [Suporte do MariaDB Audit Plugin para MySQL](#) na documentação do Amazon RDS. Os registros no registro de auditoria são armazenados em um formato específico, conforme definido pelo plug-in. Você pode encontrar mais detalhes sobre o formato do registro de auditoria na [Documentação do MariaDB Server](#).

ONuvem AWS trilha de auditoria para sua AWS conta é fornecida pelo [AWS CloudTrail](#) serviço. CloudTrail captura chamadas de API para o Amazon RDS como eventos. Todas as ações do Amazon RDS são registradas. CloudTrail fornece um registro das ações no Amazon RDS realizadas por um usuário, função ou outro AWS serviço. Os eventos incluem ações realizadas no AWS Console de gerenciamento, AWS CLI, e AWS SDKs e APIs.

Exemplo

Em um cenário de auditoria típico, talvez seja necessário combinar AWS CloudTrail trilhas com o registro de auditoria do banco de dados e o monitoramento de eventos do Amazon RDS. Por exemplo, você pode ter um cenário em que os parâmetros do banco de dados da sua instância de banco de dados Amazon RDS (por exemplo, `database-1`) foram modificados e sua tarefa é identificar quem fez a modificação, o que foi alterado e quando a mudança aconteceu.

Para realizar a tarefa, siga estas etapas:

1. Liste os eventos do Amazon RDS que aconteceram com a instância do banco de dados `database-1` e determine se há um evento na categoria `configuration change` que tem a mensagem `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 qual grupo de parâmetros de banco de dados a instância de banco de dados está usando:

```
$ 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. [Use o AWS CLI para pesquisar CloudTrail eventos](#) na região onde database-1 é implantado, no período em torno do evento Amazon RDS descoberto na etapa 1, e onde 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"
}
```

O CloudTrail evento revela que `User1` com papel `Role1` desde AWS a conta `111122223333` modificou o grupo de parâmetros do banco de dados `mariadb10-6-test`, que foi usado pela instância de banco de dados `database-1em2022-12-01` at `09:18:19` h. Dois parâmetros foram modificados e definidos com os seguintes valores:

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

AdicionalCloudTrailCloudWatchRecursos de registros

Você pode solucionar incidentes operacionais e de segurança nos últimos 90 dias visualizando `Histórico` do evento no `CloudTrail console`. Para estender o período de retenção e aproveitar os recursos adicionais de consulta, você pode usar [AWS CloudTrail Lago](#). Com `AWS CloudTrail Lake`, você pode manter os dados de eventos em um armazenamento de dados de eventos por até sete anos. Além disso, o serviço oferece suporte a consultas SQL complexas que oferecem uma visão mais profunda e personalizável dos eventos do que as visualizações fornecidas por pesquisas simples de valores-chave no `Histórico` do evento.

Para monitorar suas trilhas de auditoria, definir alarmes e receber notificações quando uma atividade específica ocorrer, você precisa [configurar CloudTrail para enviar seus registros de trilhas para CloudWatch Registros](#). Depois que os registros da trilha forem armazenados como `CloudWatch Registros`, você pode definir filtros métricos para avaliar eventos de registro para corresponder a termos, frases ou valores e atribuir métricas a filtros métricos. Além disso, você pode criar `CloudWatch alarmes` que são gerados de acordo com os limites e períodos de tempo especificados por você. Por exemplo, você pode configurar alarmes que enviam notificações às equipes responsáveis, para que elas possam tomar as medidas apropriadas. Você também pode configurar `CloudWatch` para realizar uma ação automaticamente em resposta a um alarme.

Geração de alertas

Os alertas são uma das fontes de informação mais importantes quando se trata de segurança, disponibilidade, desempenho e confiabilidade de sua infraestrutura de TI e serviços de TI. Eles notificam e informam suas equipes de TI sobre ameaças contínuas à segurança, interrupções, problemas de desempenho ou falhas no sistema.

A Biblioteca de Infraestrutura de Tecnologia da Informação (ITIL), especificamente as práticas de gerenciamento de serviços de TI (ITSM), definiu alertas automatizados como ponto focal das melhores práticas de monitoramento e gerenciamento de eventos e gerenciamento de incidentes.

O alerta de incidentes ocorre quando as ferramentas de monitoramento geram alertas para notificar sua equipe e ferramentas automatizadas (para itens que são acionáveis automaticamente) sobre mudanças, ações de alto risco ou falhas no ambiente de TI. Os alertas de TI são a primeira linha de defesa contra interrupções ou alterações do sistema que podem se transformar em grandes incidentes. Ao monitorar automaticamente os sistemas e gerar alertas de interrupções e mudanças arriscadas, as equipes de TI podem minimizar o tempo de inatividade e reduzir o alto custo decorrente disso.

Como melhores práticas, oAWSO Well-Architected Framework prescreve que você [use o monitoramento para gerar notificações baseadas em alarmes](#), e [monitore e alarme de forma proativa](#). Use CloudWatch ou um serviço de monitoramento terceirizado para definir alarmes que indicam quando as métricas estão fora dos limites esperados.

O objetivo do gerenciamento de alertas é estabelecer procedimentos eficientes e padronizados para lidar com eventos e incidentes relacionados à TI por meio de registro, classificação, definição e implementação de ações, encerramento e atividades de revisão pós-incidentes.

Seções

- Alarmes de [CloudWatch do](#)
- [EventBridge](#) regras
- [Especificando ações, ativando e desativando alarmes](#)

Alarmes do CloudWatch

Ao operar suas instâncias de banco de dados Amazon RDS, você deseja monitorar e gerar alertas sobre diferentes tipos de métricas, eventos e rastreamentos. Para bancos de dados MySQL e MariaDB, as fontes críticas de informação são [métricas da instância de banco de dados](#), [Métricas do sistema operacional](#), [eventos](#), [registros](#) e [trilhas de auditoria](#). Recomendamos que você use [CloudWatch alarmes](#) para observar uma única métrica durante um período de tempo especificado por você.

O exemplo a seguir ilustra como você pode definir um alarme que monitore o `CPUUtilization` métrica (porcentagem de utilização da CPU) em todas as suas instâncias de banco de dados Amazon RDS. Você configura o alarme para ser acionado se a utilização da CPU em qualquer instância de banco de dados for maior que 80% durante o período de avaliação 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

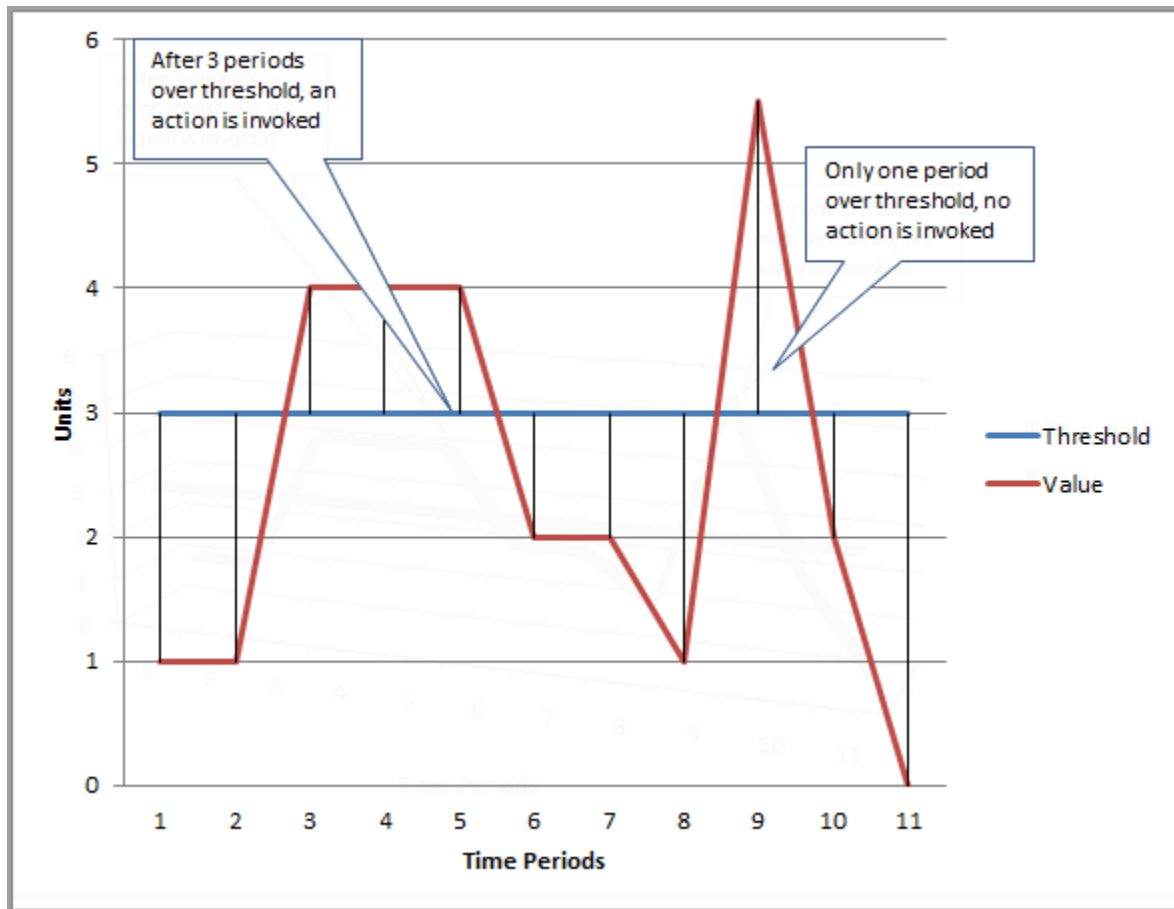
☐ **Lower**
< threshold

than...
Define the threshold value.

80

Must be a number

Isso significa que o alarme entra no **ALARM** indique se algum de seus bancos de dados experimenta uma alta utilização da CPU (mais de 80%) por 5 minutos ou mais. O alarme permanece no **OK** indique se a CPU ocasionalmente atinge mais de 80% de utilização por um curto período de tempo e, em seguida, cai novamente abaixo do limite. O gráfico a seguir ilustra essa lógica.



CloudWatchos alarmes suportam alarmes métricos e compostos.

- **UMA alarme métrico** assiste um single CloudWatch métrica e pode executar expressões matemáticas na métrica. Um alarme métrico pode enviar mensagens do Amazon SNS, que, por sua vez, podem realizar uma ou mais ações com base no valor da métrica em relação a um determinado limite em vários períodos de tempo.
- **UMA alarme composto** é baseado em uma expressão de regra, que avalia os estados de vários alarmes e entra no ALARM estado somente se todas as condições da regra forem atendidas. Normalmente, os alarmes compostos são usados para reduzir o número de alertas desnecessários. Por exemplo, você pode ter um alarme composto que contém vários alarmes métricos configurados para nunca realizar ações. O alarme composto enviaria um alerta quando todos os alarmes métricos individuais no composto já estivessem no ALARM

CloudWatchos alarmes só podem ser vigiados CloudWatch métricas. Se você quiser criar um alarme com base no erro, na consulta lenta ou nos registros gerais, você deve criar CloudWatch métricas dos registros. Você pode fazer isso conforme discutido anteriormente no [Monitoramento do SO e Eventos](#),

[registros e trilhas de auditoria](#) seções, usando filtros para [criar métricas a partir de eventos de registro](#). Da mesma forma, para alertar sobre métricas de monitoramento aprimorado, você deve criar filtros métricos no CloudWatch desde CloudWatch Registros.

Regras do EventBridge

[Eventos do Amazon RDS](#) são entregues à Amazon EventBridge, e você pode usar [EventBridge regras](#) para reagir a esses eventos. Por exemplo, você pode criar EventBridge regras que notificariam você e tomariam uma ação se uma instância de banco de dados específica fosse interrompida ou iniciada, conforme mostra a tela a seguir.

Amazon EventBridge X

Amazon EventBridge > Rules

Rules

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.

Select event bus

Event bus
Select or enter event bus name
default

Rules (2/17)

Refresh Delete Enable Edit CloudFormation Template Create rule

Search: rds 2 matches Any status < 1 ... > Settings

<input type="checkbox"/>	Name	Status	Type	Description
<input type="checkbox"/>	rds-shutdown-database-3	Enabled	Standard	
<input type="checkbox"/>	rds-startup-database-3	Enabled	Standard	

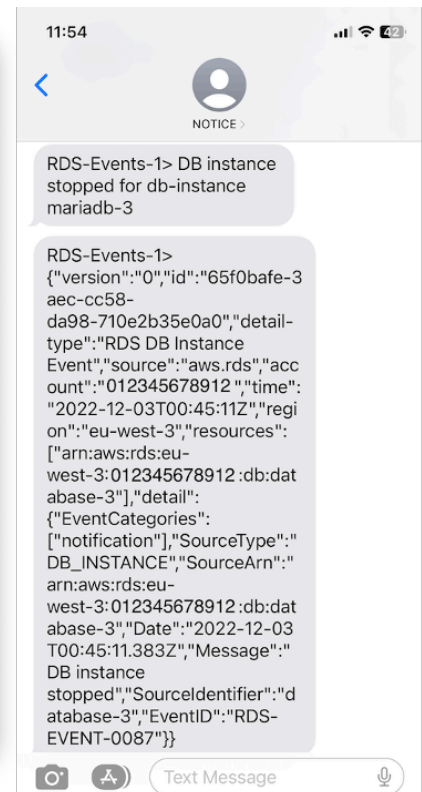
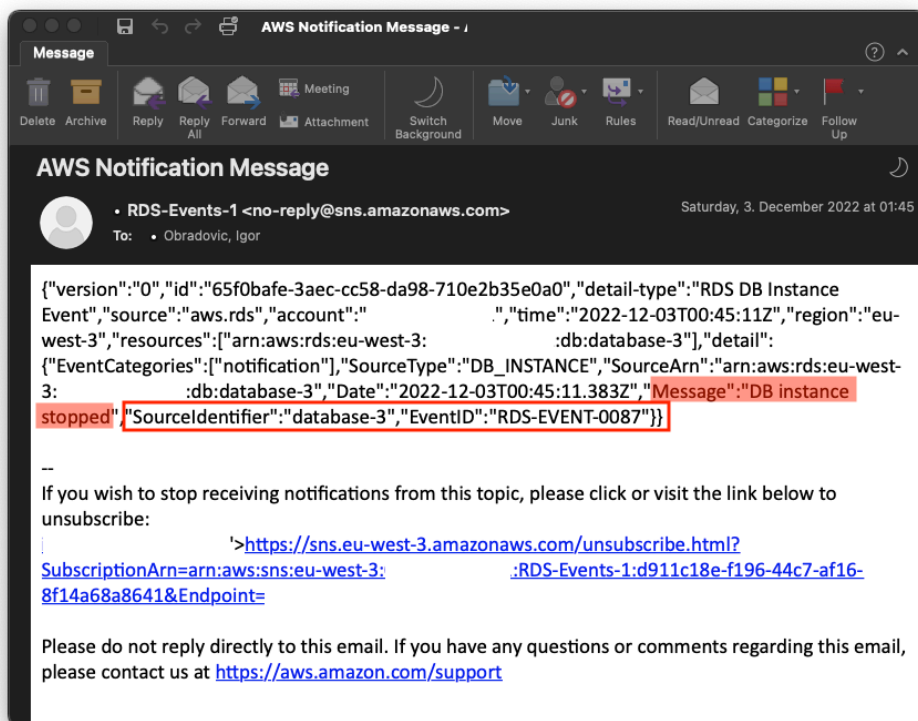
A regra que detecta `The DB instance has been stopped` evento tem o ID de evento do Amazon RDS `RDS-EVENT-0087`, então você define o `Event Pattern` propriedade da regra para:

```
{
  "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"]
  }
}
```



```
}
}
```

Essa regra monitora a instância de banco de dados `database-3` somente, e relógios para o `RDS-EVENT-0087` evento. Quando `EventBridge` detecta o evento, envia o evento para um recurso ou endpoint, conhecido como [meta](#). É aqui que você pode especificar a ação que deseja realizar se a instância do Amazon RDS for encerrada. Você pode enviar o evento para vários alvos possíveis, incluindo um tópico do SNS, uma fila do Amazon Simple Queue Service (Amazon SQS), AWS Lambda função, AWS Systems Manager Automação, uma AWS Batch trabalho, Amazon API Gateway, um plano de resposta no Incident Manager, uma capacidade de AWS Systems Manager e muitos outros. Por exemplo, você pode criar um tópico do SNS que enviará um e-mail de notificação e um SMS e atribuirá esse tópico do SNS como o destino do `EventBridge` regra. Se a instância de banco de dados Amazon RDS `database-3` foi interrompido, o Amazon RDS entrega o evento `RDS-EVENT-0087` para `EventBridge`, onde é detectado. `EventBridge` em seguida, chama o alvo, que é o tópico do SNS. O tópico SNS está configurado para enviar um e-mail (conforme mostrado na ilustração a seguir) e um SMS.



Especificando ações, ativando e desativando alarmes

Você pode usar um `CloudWatchAlarm` para especificar quais ações o alarme deve realizar quando muda entre `OK`, `ALARM`, e `INSUFFICIENT_DATA` estados. `CloudWatch` tem integração integrada com tópicos do SNS e várias categorias de ação adicionais que não são aplicáveis às métricas do Amazon RDS, como ações do Amazon Elastic Compute Cloud (Amazon EC2) ou ações em grupo do Amazon EC2 Auto Scaling. `EventBridge` geralmente é usado para escrever regras e definir alvos que realizam ações quando o alarme é acionado para métricas do Amazon RDS. `CloudWatch` envia eventos para `EventBridge` toda vez que um `CloudWatch` alarme muda seu estado. Você pode usar esses eventos de mudança de estado de alarme para acionar um alvo de evento no `EventBridge`. Para obter mais informações, consulte [Eventos de alarme e EventBridge](#) na `CloudWatch` documentação.

Talvez você também precise gerenciar alarmes; por exemplo, desabilitar automaticamente um alarme durante testes ou alterações de configuração planejadas e, em seguida, reativar o alarme quando a ação planejada terminar. Por exemplo, se você tiver uma atualização planejada e programada do software do banco de dados que exija tempo de inatividade e tiver alarmes que serão ativados se o banco de dados ficar indisponível, você poderá desativar e habilitar os alarmes usando as ações da API [DisableAlarmAction](#) e [EnableAlarmActions](#), ou o `disable-alarm-action` e `enable-alarm-actions` comandos no AWS CLI. Você também pode ver o histórico do alarme no `CloudWatch` console ou usando o [DescribeAlarmHistory](#) Ação da API ou o `describe-alarm-history` comando no AWS CLI. O `CloudWatch` preserva o histórico do alarme por duas semanas. No `CloudWatch` console, você pode escolher o `Favoritos e recentes` menu no painel de navegação para definir e acessar seus alarmes favoritos e os mais visitados recentemente.

Próximas etapas e recursos

Para obter mais informações sobre como migrar seus bancos de dados relacionais para a Nuvem AWS, veja a seguinte estratégia no AWS Site de orientação prescritiva:

- [Estratégia de migração para bancos de dados relacionais](#)

Você pode explorar [padrões de migração de banco de dados](#) pelas [step-by-step instruções](#) sobre seus bancos de dados relacionais específicos em execução na Nuvem AWS, incluindo tarefas relacionadas ao monitoramento, migração e gerenciamento de dados.

Use os filtros dessa página para encontrar padrões por AWS serviço (por exemplo, migrações para o Amazon RDS ou o Amazon Aurora), por carga de trabalho (por exemplo, de código aberto, que inclui bancos de dados MySQL e MariaDB) ou por uso planejado (produção ou piloto).

Para obter recursos adicionais, consulte o seguinte:

- [Guia do usuário do Amazon Relational Database Service](#)
- [Amazon CloudWatch Guia do usuário](#)
- [Perguntas frequentes sobre o Amazon RDS](#)
- [Perguntas frequentes sobre o Performance Insights](#)
- [Entregue métricas de contador do Amazon RDS Performance Insights a um provedor terceirizado de serviços de monitoramento de desempenho de aplicativos usando a Amazon CloudWatch Fluxo de métricas](#) (AWSpostagem no blog)
- [Criando uma Amazon CloudWatch painel para monitorar o Amazon RDS e o Amazon Aurora MySQL](#) (AWSpostagem no blog)
- [Ajustando o Amazon RDS para MySQL com Performance Insights](#) (AWSpostagem no blog)

Histórico do documento

A tabela a seguir descreve alterações significativas feitas neste guia. Se desejar receber notificações sobre futuras atualizações, inscreva-se em um [feed RSS](#).

Alteração	Descrição	Data
Informações atualizadas	Atualizou as informações sobre exportadores e adicionou diretrizes para escolher um exportador.	13 de junho de 2024
Publicação inicial	—	30 de junho de 2023

AWS Glossário de orientação prescritiva

A seguir estão os termos comumente usados em estratégias, guias e padrões fornecidos pela Orientação AWS Prescritiva. Para sugerir entradas, use o link Fornecer feedback no final do glossário.

Números

7 Rs

Sete estratégias comuns de migração para mover aplicações para a nuvem. Essas estratégias baseiam-se nos 5 Rs identificados pela Gartner em 2011 e consistem em:

- Refatorar/rearquitetar: mova uma aplicação e modifique sua arquitetura aproveitando ao máximo os recursos nativos de nuvem para melhorar a agilidade, a performance e a escalabilidade. Isso normalmente envolve a portabilidade do sistema operacional e do banco de dados. Exemplo: migrar seu banco de dados Oracle on-premises para o Amazon Aurora Edição Compatível com PostgreSQL.
- Redefinir a plataforma (mover e redefinir [mover e redefinir (lift-and-reshape)]): mova uma aplicação para a nuvem e introduza algum nível de otimização a fim de aproveitar os recursos da nuvem. Exemplo: migre seu banco de dados Oracle local para o Amazon Relational Database Service (Amazon RDS) para Oracle na nuvem. AWS
- Recomprar (drop and shop): mude para um produto diferente, normalmente migrando de uma licença tradicional para um modelo SaaS. Exemplo: migrar seu sistema de gerenciamento de relacionamento com o cliente (CRM) para o Salesforce.com.
- Redefinir a hospedagem (mover sem alterações [lift-and-shift])mover uma aplicação para a nuvem sem fazer nenhuma alteração a fim de aproveitar os recursos da nuvem. Exemplo: migre seu banco de dados Oracle local para o Oracle em uma instância do EC2 na nuvem. AWS
- Realocar (mover o hipervisor sem alterações [hypervisor-level lift-and-shift]): mover a infraestrutura para a nuvem sem comprar novo hardware, reescrever aplicações ou modificar suas operações existentes. Esse cenário de migração é específico do VMware Cloud on AWS, que oferece suporte à compatibilidade de máquinas virtuais (VM) e à portabilidade da carga de trabalho entre seu ambiente local e. AWSÉ possível usar as tecnologias VMware Cloud Foundation de seus datacenters on-premises ao migrar sua infraestrutura para o VMware

Cloud na AWS. Exemplo: realocar o hipervisor que hospeda seu banco de dados Oracle para o VMware Cloud on. AWS

- Reter (revisitar): mantenha as aplicações em seu ambiente de origem. Isso pode incluir aplicações que exigem grande refatoração, e você deseja adiar esse trabalho para um momento posterior, e aplicações antigas que você deseja manter porque não há justificativa comercial para migrá-las.
- Retirar: desative ou remova aplicações que não são mais necessárias em seu ambiente de origem.

A

ABAC

Consulte controle de [acesso baseado em atributos](#).

serviços abstratos

Veja os [serviços gerenciados](#).

ACID

Veja [atomicidade, consistência, isolamento, durabilidade](#).

migração ativa-ativa

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia (por meio de uma ferramenta de replicação bidirecional ou operações de gravação dupla), e ambos os bancos de dados lidam com transações de aplicações conectadas durante a migração. Esse método oferece suporte à migração em lotes pequenos e controlados, em vez de exigir uma substituição única. É mais flexível, mas exige mais trabalho do que a migração [ativa-passiva](#).

migração ativa-passiva

Um método de migração de banco de dados no qual os bancos de dados de origem e de destino são mantidos em sincronia, mas somente o banco de dados de origem manipula as transações das aplicações conectadas enquanto os dados são replicados no banco de dados de destino. O banco de dados de destino não aceita nenhuma transação durante a migração.

função agregada

Uma função SQL que opera em um grupo de linhas e calcula um único valor de retorno para o grupo. Exemplos de funções agregadas incluem SUM e MAX.

AI

Veja [inteligência artificial](#).

AIOps

Veja as [operações de inteligência artificial](#).

anonimização

O processo de excluir permanentemente informações pessoais em um conjunto de dados. A anonimização pode ajudar a proteger a privacidade pessoal. Dados anônimos não são mais considerados dados pessoais.

antipadrões

Uma solução frequentemente usada para um problema recorrente em que a solução é contraproducente, ineficaz ou menos eficaz do que uma alternativa.

controle de aplicativos

Uma abordagem de segurança que permite o uso somente de aplicativos aprovados para ajudar a proteger um sistema contra malware.

portfólio de aplicações

Uma coleção de informações detalhadas sobre cada aplicação usada por uma organização, incluindo o custo para criar e manter a aplicação e seu valor comercial. Essas informações são fundamentais para [o processo de descoberta e análise de portfólio](#) e ajudam a identificar e priorizar as aplicações a serem migradas, modernizadas e otimizadas.

inteligência artificial (IA)

O campo da ciência da computação que se dedica ao uso de tecnologias de computação para desempenhar funções cognitivas normalmente associadas aos humanos, como aprender, resolver problemas e reconhecer padrões. Para obter mais informações, consulte [O que é inteligência artificial?](#)

operações de inteligência artificial (AIOps)

O processo de usar técnicas de machine learning para resolver problemas operacionais, reduzir incidentes operacionais e intervenção humana e aumentar a qualidade do serviço. Para obter

mais informações sobre como as AIOps são usadas na estratégia de migração para a AWS , consulte o [guia de integração de operações](#).

criptografia assimétrica

Um algoritmo de criptografia que usa um par de chaves, uma chave pública para criptografia e uma chave privada para descriptografia. É possível compartilhar a chave pública porque ela não é usada na descriptografia, mas o acesso à chave privada deve ser altamente restrito.

atomicidade, consistência, isolamento, durabilidade (ACID)

Um conjunto de propriedades de software que garantem a validade dos dados e a confiabilidade operacional de um banco de dados, mesmo no caso de erros, falhas de energia ou outros problemas.

controle de acesso por atributo (ABAC)

A prática de criar permissões minuciosas com base nos atributos do usuário, como departamento, cargo e nome da equipe. Para obter mais informações, consulte [ABAC AWS](#) na documentação AWS Identity and Access Management (IAM).

fonte de dados autorizada

Um local onde você armazena a versão principal dos dados, que é considerada a fonte de informações mais confiável. Você pode copiar dados da fonte de dados autorizada para outros locais com o objetivo de processar ou modificar os dados, como anonimizá-los, redigi-los ou pseudonimizá-los.

Availability Zone (zona de disponibilidade)

Um local distinto dentro de um Região da AWS que está isolado de falhas em outras zonas de disponibilidade e fornece conectividade de rede barata e de baixa latência a outras zonas de disponibilidade na mesma região.

AWS Estrutura de adoção da nuvem (AWS CAF)

Uma estrutura de diretrizes e melhores práticas AWS para ajudar as organizações a desenvolver um plano eficiente e eficaz para migrar com sucesso para a nuvem. AWS O CAF organiza a orientação em seis áreas de foco chamadas perspectivas: negócios, pessoas, governança, plataforma, segurança e operações. As perspectivas de negócios, pessoas e governança têm como foco habilidades e processos de negócios; as perspectivas de plataforma, segurança e operações concentram-se em habilidades e processos técnicos. Por exemplo, a perspectiva das pessoas tem como alvo as partes interessadas que lidam com recursos humanos (RH), funções de pessoal e gerenciamento de pessoal. Nessa perspectiva, o AWS CAF fornece orientação para

desenvolvimento, treinamento e comunicação de pessoas para ajudar a preparar a organização para a adoção bem-sucedida da nuvem. Para obter mais informações, consulte o [site da AWS CAF](#) e o [whitepaper da AWS CAF](#).

AWS Estrutura de qualificação da carga de trabalho (AWS WQF)

Uma ferramenta que avalia as cargas de trabalho de migração do banco de dados, recomenda estratégias de migração e fornece estimativas de trabalho. AWS O WQF está incluído com AWS Schema Conversion Tool (AWS SCT). Ela analisa esquemas de banco de dados e objetos de código, código de aplicações, dependências e características de performance, além de fornecer relatórios de avaliação.

B

bot ruim

Um [bot](#) destinado a perturbar ou causar danos a indivíduos ou organizações.

BCP

Veja o [planejamento de continuidade de negócios](#).

gráfico de comportamento

Uma visualização unificada e interativa do comportamento e das interações de recursos ao longo do tempo. É possível usar um gráfico de comportamento com o Amazon Detective para examinar tentativas de login malsucedidas, chamadas de API suspeitas e ações similares. Para obter mais informações, consulte [Dados em um gráfico de comportamento](#) na documentação do Detective.

sistema big-endian

Um sistema que armazena o byte mais significativo antes. Veja também [endianness](#).

classificação binária

Um processo que prevê um resultado binário (uma de duas classes possíveis). Por exemplo, seu modelo de ML pode precisar prever problemas como “Este e-mail é ou não é spam?” ou “Este produto é um livro ou um carro?”

filtro de bloom

Uma estrutura de dados probabilística e eficiente em termos de memória que é usada para testar se um elemento é membro de um conjunto.

blue/green deployment (implantação azul/verde)

Uma estratégia de implantação em que você cria dois ambientes separados, mas idênticos. Você executa a versão atual do aplicativo em um ambiente (azul) e a nova versão do aplicativo no outro ambiente (verde). Essa estratégia ajuda você a reverter rapidamente com o mínimo de impacto.

bot

Um aplicativo de software que executa tarefas automatizadas pela Internet e simula a atividade ou interação humana. Alguns bots são úteis ou benéficos, como rastreadores da Web que indexam informações na Internet. Alguns outros bots, conhecidos como bots ruins, têm como objetivo perturbar ou causar danos a indivíduos ou organizações.

botnet

Redes de [bots](#) infectadas por [malware](#) e sob o controle de uma única parte, conhecidas como pastor de bots ou operador de bots. As redes de bots são o mecanismo mais conhecido para escalar bots e seu impacto.

ramo

Uma área contida de um repositório de código. A primeira ramificação criada em um repositório é a ramificação principal. Você pode criar uma nova ramificação a partir de uma ramificação existente e, em seguida, desenvolver recursos ou corrigir bugs na nova ramificação. Uma ramificação que você cria para gerar um recurso é comumente chamada de ramificação de recurso. Quando o recurso estiver pronto para lançamento, você mesclará a ramificação do recurso de volta com a ramificação principal. Para obter mais informações, consulte [Sobre filiais](#) (GitHub documentação).

acesso em vidro quebrado

Em circunstâncias excepcionais e por meio de um processo aprovado, um meio rápido para um usuário obter acesso a um Conta da AWS que ele normalmente não tem permissão para acessar. Para obter mais informações, consulte o indicador [Implementar procedimentos de quebra de vidro na orientação do Well-Architected AWS](#).

estratégia brownfield

A infraestrutura existente em seu ambiente. Ao adotar uma estratégia brownfield para uma arquitetura de sistema, você desenvolve a arquitetura de acordo com as restrições dos sistemas e da infraestrutura atuais. Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e [greenfield](#).

cache do buffer

A área da memória em que os dados acessados com mais frequência são armazenados.

capacidade de negócios

O que uma empresa faz para gerar valor (por exemplo, vendas, atendimento ao cliente ou marketing). As arquiteturas de microsserviços e as decisões de desenvolvimento podem ser orientadas por recursos de negócios. Para obter mais informações, consulte a seção [Organizados de acordo com as capacidades de negócios](#) do whitepaper [Executar microsserviços containerizados na AWS](#).

planejamento de continuidade de negócios (BCP)

Um plano que aborda o impacto potencial de um evento disruptivo, como uma migração em grande escala, nas operações e permite que uma empresa retome as operações rapidamente.

C

CAF

Consulte [Estrutura de adoção da AWS nuvem](#).

implantação canária

O lançamento lento e incremental de uma versão para usuários finais. Quando estiver confiante, você implanta a nova versão e substituirá a versão atual em sua totalidade.

CCoE

Veja o [Centro de Excelência em Nuvem](#).

CDC

Veja [a captura de dados de alterações](#).

captura de dados de alterações (CDC)

O processo de rastrear alterações em uma fonte de dados, como uma tabela de banco de dados, e registrar metadados sobre a alteração. É possível usar o CDC para várias finalidades, como auditar ou replicar alterações em um sistema de destino para manter a sincronização.

engenharia do caos

Introduzir intencionalmente falhas ou eventos disruptivos para testar a resiliência de um sistema. Você pode usar [AWS Fault Injection Service \(AWS FIS\)](#) para realizar experimentos que estressam suas AWS cargas de trabalho e avaliar sua resposta.

CI/CD

Veja a [integração e a entrega contínuas](#).

classificação

Um processo de categorização que ajuda a gerar previsões. Os modelos de ML para problemas de classificação predizem um valor discreto. Os valores discretos são sempre diferentes uns dos outros. Por exemplo, um modelo pode precisar avaliar se há ou não um carro em uma imagem.

criptografia no lado do cliente

Criptografia de dados localmente, antes que o alvo os AWS service (Serviço da AWS) receba.

Centro de Excelência da Nuvem (CCoE)

Uma equipe multidisciplinar que impulsiona os esforços de adoção da nuvem em toda a organização, incluindo o desenvolvimento de práticas recomendadas de nuvem, a mobilização de recursos, o estabelecimento de cronogramas de migração e a liderança da organização em transformações em grande escala. Para obter mais informações, consulte as [postagens do CCoE no blog](#) AWS Cloud Enterprise Strategy.

computação em nuvem

A tecnologia de nuvem normalmente usada para armazenamento de dados remoto e gerenciamento de dispositivos de IoT. A computação em nuvem geralmente está conectada à tecnologia de [computação de ponta](#).

modelo operacional em nuvem

Em uma organização de TI, o modelo operacional usado para criar, amadurecer e otimizar um ou mais ambientes de nuvem. Para obter mais informações, consulte [Criar seu modelo operacional de nuvem](#).

estágios de adoção da nuvem

As quatro fases pelas quais as organizações normalmente passam quando migram para a AWS nuvem:

- Projeto: executar alguns projetos relacionados à nuvem para fins de prova de conceito e aprendizado
- Fundação: realizar investimentos fundamentais para escalar sua adoção da nuvem (por exemplo, criar uma zona de pouso, definir um CCoE, estabelecer um modelo de operações)
- Migração: migrar aplicações individuais
- Reinvenção: otimizar produtos e serviços e inovar na nuvem

Esses estágios foram definidos por Stephen Orban na postagem do blog [The Journey Toward Cloud-First & the Stages of Adoption](#) no blog AWS Cloud Enterprise Strategy. Para obter informações sobre como eles se relacionam com a estratégia de AWS migração, consulte o [guia de preparação para migração](#).

CMDB

Consulte o [banco de dados de gerenciamento de configuração](#).

repositório de código

Um local onde o código-fonte e outros ativos, como documentação, amostras e scripts, são armazenados e atualizados por meio de processos de controle de versão. Os repositórios de nuvem comuns incluem GitHub ou AWS CodeCommit. Cada versão do código é chamada de ramificação. Em uma estrutura de microsserviços, cada repositório é dedicado a uma única peça de funcionalidade. Um único pipeline de CI/CD pode usar vários repositórios.

cache frio

Um cache de buffer que está vazio, não está bem preenchido ou contém dados obsoletos ou irrelevantes. Isso afeta a performance porque a instância do banco de dados deve ler da memória principal ou do disco, um processo que é mais lento do que a leitura do cache do buffer.

dados frios

Dados que raramente são acessados e geralmente são históricos. Ao consultar esse tipo de dados, consultas lentas geralmente são aceitáveis. Mover esses dados para níveis ou classes de armazenamento de baixo desempenho e menos caros pode reduzir os custos.

visão computacional (CV)

Um campo da [IA](#) que usa aprendizado de máquina para analisar e extrair informações de formatos visuais, como imagens e vídeos digitais. Por exemplo, AWS Panorama oferece dispositivos que adicionam CV às redes de câmeras locais, e a Amazon SageMaker fornece algoritmos de processamento de imagem para CV.

desvio de configuração

Para uma carga de trabalho, uma alteração de configuração em relação ao estado esperado. Isso pode fazer com que a carga de trabalho se torne incompatível e, normalmente, é gradual e não intencional.

banco de dados de gerenciamento de configuração (CMDB)

Um repositório que armazena e gerencia informações sobre um banco de dados e seu ambiente de TI, incluindo componentes de hardware e software e suas configurações. Normalmente, os dados de um CMDB são usados no estágio de descoberta e análise do portfólio da migração.

pacote de conformidade

Um conjunto de AWS Config regras e ações de remediação que você pode montar para personalizar suas verificações de conformidade e segurança. Você pode implantar um pacote de conformidade como uma entidade única em uma Conta da AWS região ou em uma organização usando um modelo YAML. Para obter mais informações, consulte [Pacotes de conformidade na documentação](#). AWS Config

integração contínua e entrega contínua (CI/CD)

O processo de automatizar os estágios de origem, criação, teste, preparação e produção do processo de lançamento do software. O CI/CD é comumente descrito como um pipeline. O CI/CD pode ajudar você a automatizar processos, melhorar a produtividade, melhorar a qualidade do código e entregar com mais rapidez. Para obter mais informações, consulte [Benefícios da entrega contínua](#). CD também pode significar implantação contínua. Para obter mais informações, consulte [Entrega contínua versus implantação contínua](#).

CV

Veja [visão computacional](#).

D

dados em repouso

Dados estacionários em sua rede, por exemplo, dados que estão em um armazenamento.

classificação de dados

Um processo para identificar e categorizar os dados em sua rede com base em criticalidade e confidencialidade. É um componente crítico de qualquer estratégia de gerenciamento de riscos de

segurança cibernética, pois ajuda a determinar os controles adequados de proteção e retenção para os dados. A classificação de dados é um componente do pilar de segurança no AWS Well-Architected Framework. Para obter mais informações, consulte [Classificação de dados](#).

desvio de dados

Uma variação significativa entre os dados de produção e os dados usados para treinar um modelo de ML ou uma alteração significativa nos dados de entrada ao longo do tempo. O desvio de dados pode reduzir a qualidade geral, a precisão e a imparcialidade das previsões do modelo de ML.

dados em trânsito

Dados que estão se movendo ativamente pela sua rede, como entre os recursos da rede.

malha de dados

Uma estrutura arquitetônica que fornece propriedade de dados distribuída e descentralizada com gerenciamento e governança centralizados.

minimização de dados

O princípio de coletar e processar apenas os dados estritamente necessários. Praticar a minimização de dados no Nuvem AWS pode reduzir os riscos de privacidade, os custos e a pegada de carbono de sua análise.

perímetro de dados

Um conjunto de proteções preventivas em seu AWS ambiente que ajudam a garantir que somente identidades confiáveis acessem recursos confiáveis das redes esperadas. Para obter mais informações, consulte [Construindo um perímetro de dados em AWS](#)

pré-processamento de dados

A transformação de dados brutos em um formato que seja facilmente analisado por seu modelo de ML. O pré-processamento de dados pode significar a remoção de determinadas colunas ou linhas e o tratamento de valores ausentes, inconsistentes ou duplicados.

proveniência dos dados

O processo de rastrear a origem e o histórico dos dados ao longo de seu ciclo de vida, por exemplo, como os dados foram gerados, transmitidos e armazenados.

titular dos dados

Um indivíduo cujos dados estão sendo coletados e processados.

data warehouse

Um sistema de gerenciamento de dados que oferece suporte à inteligência comercial, como análises. Os data warehouses geralmente contêm grandes quantidades de dados históricos e geralmente são usados para consultas e análises.

linguagem de definição de dados (DDL)

Instruções ou comandos para criar ou modificar a estrutura de tabelas e objetos em um banco de dados.

linguagem de manipulação de dados (DML)

Instruções ou comandos para modificar (inserir, atualizar e excluir) informações em um banco de dados.

DDL

Consulte a [linguagem de definição de banco](#) de dados.

deep ensemble

A combinação de vários modelos de aprendizado profundo para gerar previsões. Os deep ensembles podem ser usados para produzir uma previsão mais precisa ou para estimar a incerteza nas previsões.

Aprendizado profundo

Um subcampo do ML que usa várias camadas de redes neurais artificiais para identificar o mapeamento entre os dados de entrada e as variáveis-alvo de interesse.

defense-in-depth

Uma abordagem de segurança da informação na qual uma série de mecanismos e controles de segurança são cuidadosamente distribuídos por toda a rede de computadores para proteger a confidencialidade, a integridade e a disponibilidade da rede e dos dados nela contidos. Ao adotar essa estratégia AWS, você adiciona vários controles em diferentes camadas da AWS Organizations estrutura para ajudar a proteger os recursos. Por exemplo, uma defense-in-depth abordagem pode combinar autenticação multifatorial, segmentação de rede e criptografia.

administrador delegado

Em AWS Organizations, um serviço compatível pode registrar uma conta de AWS membro para administrar as contas da organização e gerenciar as permissões desse serviço. Essa conta

é chamada de administrador delegado para esse serviço. Para obter mais informações e uma lista de serviços compatíveis, consulte [Serviços que funcionam com o AWS Organizations](#) na documentação do AWS Organizations .

implantação

O processo de criar uma aplicação, novos recursos ou correções de código disponíveis no ambiente de destino. A implantação envolve a implementação de mudanças em uma base de código e, em seguida, a criação e execução dessa base de código nos ambientes da aplicação.

ambiente de desenvolvimento

Veja o [ambiente](#).

controle detectivo

Um controle de segurança projetado para detectar, registrar e alertar após a ocorrência de um evento. Esses controles são uma segunda linha de defesa, alertando você sobre eventos de segurança que contornaram os controles preventivos em vigor. Para obter mais informações, consulte [Controles detectivos](#) em Como implementar controles de segurança na AWS.

mapeamento do fluxo de valor de desenvolvimento (DVSM)

Um processo usado para identificar e priorizar restrições que afetam negativamente a velocidade e a qualidade em um ciclo de vida de desenvolvimento de software. O DVSM estende o processo de mapeamento do fluxo de valor originalmente projetado para práticas de manufatura enxuta. Ele se concentra nas etapas e equipes necessárias para criar e movimentar valor por meio do processo de desenvolvimento de software.

gêmeo digital

Uma representação virtual de um sistema real, como um prédio, fábrica, equipamento industrial ou linha de produção. Os gêmeos digitais oferecem suporte à manutenção preditiva, ao monitoramento remoto e à otimização da produção.

tabela de dimensões

Em um [esquema em estrela](#), uma tabela menor que contém atributos de dados sobre dados quantitativos em uma tabela de fatos. Os atributos da tabela de dimensões geralmente são campos de texto ou números discretos que se comportam como texto. Esses atributos são comumente usados para restringir consultas, filtrar e rotular conjuntos de resultados.

desastre

Um evento que impede que uma workload ou sistema cumpra seus objetivos de negócios em seu local principal de implantação. Esses eventos podem ser desastres naturais, falhas técnicas ou o resultado de ações humanas, como configuração incorreta não intencional ou ataque de malware.

recuperação de desastres (DR)

A estratégia e o processo que você usa para minimizar o tempo de inatividade e a perda de dados causados por um [desastre](#). Para obter mais informações, consulte [Recuperação de desastres de cargas de trabalho em AWS: Recuperação na nuvem no AWS Well-Architected Framework](#).

DML

Consulte [linguagem de manipulação de banco](#) de dados.

design orientado por domínio

Uma abordagem ao desenvolvimento de um sistema de software complexo conectando seus componentes aos domínios em evolução, ou principais metas de negócios, atendidos por cada componente. Esse conceito foi introduzido por Eric Evans em seu livro, Design orientado por domínio: lidando com a complexidade no coração do software (Boston: Addison-Wesley Professional, 2003). Para obter informações sobre como usar o design orientado por domínio com o padrão strangler fig, consulte [Modernizar incrementalmente os serviços web herdados do Microsoft ASP.NET \(ASMX\) usando contêineres e o Amazon API Gateway](#).

DR

Veja a [recuperação de desastres](#).

detecção de deriva

Rastreando desvios de uma configuração básica. Por exemplo, você pode usar AWS CloudFormation para [detectar desvios nos recursos do sistema](#) ou AWS Control Tower para [detectar mudanças em seu landing zone](#) que possam afetar a conformidade com os requisitos de governança.

DVSM

Veja o [mapeamento do fluxo de valor do desenvolvimento](#).

E

EDA

Veja a [análise exploratória de dados](#).

computação de borda

A tecnologia que aumenta o poder computacional de dispositivos inteligentes nas bordas de uma rede de IoT. Quando comparada à [computação em nuvem](#), a computação de ponta pode reduzir a latência da comunicação e melhorar o tempo de resposta.

Criptografia

Um processo de computação que transforma dados de texto simples, legíveis por humanos, em texto cifrado.

chave de criptografia

Uma sequência criptográfica de bits aleatórios que é gerada por um algoritmo de criptografia. As chaves podem variar em tamanho, e cada chave foi projetada para ser imprevisível e exclusiva.

endianismo

A ordem na qual os bytes são armazenados na memória do computador. Os sistemas big-endian armazenam o byte mais significativo antes. Os sistemas little-endian armazenam o byte menos significativo antes.

endpoint

Veja o [endpoint do serviço](#).

serviço de endpoint

Um serviço que pode ser hospedado em uma nuvem privada virtual (VPC) para ser compartilhado com outros usuários. Você pode criar um serviço de endpoint com AWS PrivateLink e conceder permissões a outros diretores Contas da AWS ou a AWS Identity and Access Management (IAM). Essas contas ou entidades principais podem se conectar ao serviço de endpoint de maneira privada criando endpoints da VPC de interface. Para obter mais informações, consulte [Criar um serviço de endpoint](#) na documentação do Amazon Virtual Private Cloud (Amazon VPC).

planejamento de recursos corporativos (ERP)

Um sistema que automatiza e gerencia os principais processos de negócios (como contabilidade, [MES](#) e gerenciamento de projetos) para uma empresa.

criptografia envelopada

O processo de criptografar uma chave de criptografia com outra chave de criptografia. Para obter mais informações, consulte [Criptografia de envelope](#) na documentação AWS Key Management Service (AWS KMS).

environment (ambiente)

Uma instância de uma aplicação em execução. Estes são tipos comuns de ambientes na computação em nuvem:

- ambiente de desenvolvimento: uma instância de uma aplicação em execução que está disponível somente para a equipe principal responsável pela manutenção da aplicação. Ambientes de desenvolvimento são usados para testar mudanças antes de promovê-las para ambientes superiores. Esse tipo de ambiente às vezes é chamado de ambiente de teste.
- ambientes inferiores: todos os ambientes de desenvolvimento para uma aplicação, como aqueles usados para compilações e testes iniciais.
- ambiente de produção: uma instância de uma aplicação em execução que os usuários finais podem acessar. Em um pipeline de CI/CD, o ambiente de produção é o último ambiente de implantação.
- ambientes superiores: todos os ambientes que podem ser acessados por usuários que não sejam a equipe principal de desenvolvimento. Isso pode incluir um ambiente de produção, ambientes de pré-produção e ambientes para testes de aceitação do usuário.

epic

Em metodologias ágeis, categorias funcionais que ajudam a organizar e priorizar seu trabalho. Os epics fornecem uma descrição de alto nível dos requisitos e das tarefas de implementação. Por exemplo, os épicos de segurança AWS da CAF incluem gerenciamento de identidade e acesso, controles de detetive, segurança de infraestrutura, proteção de dados e resposta a incidentes. Para obter mais informações sobre epics na estratégia de migração da AWS, consulte o [guia de implementação do programa](#).

ERP

Consulte [planejamento de recursos corporativos](#).

análise exploratória de dados (EDA)

O processo de analisar um conjunto de dados para entender suas principais características. Você coleta ou agrega dados e, em seguida, realiza investigações iniciais para encontrar padrões,

detectar anomalias e verificar suposições. O EDA é realizado por meio do cálculo de estatísticas resumidas e da criação de visualizações de dados.

F

tabela de fatos

A tabela central em um [esquema em estrela](#). Ele armazena dados quantitativos sobre operações comerciais. Normalmente, uma tabela de fatos contém dois tipos de colunas: aquelas que contêm medidas e aquelas que contêm uma chave externa para uma tabela de dimensões.

falham rapidamente

Uma filosofia que usa testes frequentes e incrementais para reduzir o ciclo de vida do desenvolvimento. É uma parte essencial de uma abordagem ágil.

limite de isolamento de falhas

No Nuvem AWS, um limite, como uma zona de disponibilidade, Região da AWS um plano de controle ou um plano de dados, que limita o efeito de uma falha e ajuda a melhorar a resiliência das cargas de trabalho. Para obter mais informações, consulte [Limites de isolamento de AWS falhas](#).

ramificação de recursos

Veja a [filial](#).

recursos

Os dados de entrada usados para fazer uma previsão. Por exemplo, em um contexto de manufatura, os recursos podem ser imagens capturadas periodicamente na linha de fabricação.

importância do recurso

O quanto um recurso é importante para as previsões de um modelo. Isso geralmente é expresso como uma pontuação numérica que pode ser calculada por meio de várias técnicas, como Shapley Additive Explanations (SHAP) e gradientes integrados. Para obter mais informações, consulte [Interpretabilidade do modelo de aprendizado de máquina com:AWS](#).

transformação de recursos

O processo de otimizar dados para o processo de ML, incluindo enriquecer dados com fontes adicionais, escalar valores ou extrair vários conjuntos de informações de um único

campo de dados. Isso permite que o modelo de ML se beneficie dos dados. Por exemplo, se a data “2021-05-27 00:15:37” for dividida em “2021”, “maio”, “quinta” e “15”, isso poderá ajudar o algoritmo de aprendizado a aprender padrões diferenciados associados a diferentes componentes de dados.

FGAC

Veja o [controle de acesso refinado](#).

controle de acesso refinado (FGAC)

O uso de várias condições para permitir ou negar uma solicitação de acesso.

migração flash-cut

Um método de migração de banco de dados que usa replicação contínua de dados por meio da [captura de dados alterados](#) para migrar dados no menor tempo possível, em vez de usar uma abordagem em fases. O objetivo é reduzir ao mínimo o tempo de inatividade.

G

bloqueio geográfico

Veja as [restrições geográficas](#).

restrições geográficas (bloqueio geográfico)

Na Amazon CloudFront, uma opção para impedir que usuários em países específicos acessem distribuições de conteúdo. É possível usar uma lista de permissões ou uma lista de bloqueios para especificar países aprovados e banidos. Para obter mais informações, consulte [Restringir a distribuição geográfica do seu conteúdo](#) na CloudFront documentação.

Fluxo de trabalho do GitFlow

Uma abordagem na qual ambientes inferiores e superiores usam ramificações diferentes em um repositório de código-fonte. O fluxo de trabalho do Gitflow é considerado legado, e o fluxo de [trabalho baseado em troncos](#) é a abordagem moderna e preferida.

estratégia greenfield

A ausência de infraestrutura existente em um novo ambiente. Ao adotar uma estratégia greenfield para uma arquitetura de sistema, é possível selecionar todas as novas tecnologias sem a

restrição da compatibilidade com a infraestrutura existente, também conhecida como [brownfield](#). Se estiver expandindo a infraestrutura existente, poderá combinar as estratégias brownfield e greenfield.

barreira de proteção

Uma regra de alto nível que ajuda a gerenciar recursos, políticas e conformidade em todas as unidades organizacionais (UOs). Barreiras de proteção preventivas impõem políticas para garantir o alinhamento a padrões de conformidade. Elas são implementadas usando políticas de controle de serviço e limites de permissões do IAM. Barreiras de proteção detectivas detectam violações de políticas e problemas de conformidade e geram alertas para remediação. Eles são implementados usando AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector e verificações personalizadas AWS Lambda .

H

HA

Veja a [alta disponibilidade](#).

migração heterogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que usa um mecanismo de banco de dados diferente (por exemplo, Oracle para Amazon Aurora). A migração heterogênea geralmente faz parte de um esforço de redefinição da arquitetura, e converter o esquema pode ser uma tarefa complexa. [O AWS fornece o AWS SCT](#) para ajudar nas conversões de esquemas.

alta disponibilidade (HA)

A capacidade de uma workload operar continuamente, sem intervenção, em caso de desafios ou desastres. Os sistemas AH são projetados para realizar o failover automático, oferecer consistentemente desempenho de alta qualidade e lidar com diferentes cargas e falhas com impacto mínimo no desempenho.

modernização de historiador

Uma abordagem usada para modernizar e atualizar os sistemas de tecnologia operacional (OT) para melhor atender às necessidades do setor de manufatura. Um historiador é um tipo de banco de dados usado para coletar e armazenar dados de várias fontes em uma fábrica.

migração homogênea de bancos de dados

Migrar seu banco de dados de origem para um banco de dados de destino que compartilha o mesmo mecanismo de banco de dados (por exemplo, Microsoft SQL Server para Amazon RDS para SQL Server). A migração homogênea geralmente faz parte de um esforço de redefinição da hospedagem ou da plataforma. É possível usar utilitários de banco de dados nativos para migrar o esquema.

dados quentes

Dados acessados com frequência, como dados em tempo real ou dados translacionais recentes. Esses dados normalmente exigem uma camada ou classe de armazenamento de alto desempenho para fornecer respostas rápidas às consultas.

hotfix

Uma correção urgente para um problema crítico em um ambiente de produção. Devido à sua urgência, um hotfix geralmente é feito fora do fluxo de trabalho normal de DevOps lançamento.

período de hipercuidados

Imediatamente após a substituição, o período em que uma equipe de migração gerencia e monitora as aplicações migradas na nuvem para resolver quaisquer problemas. Normalmente, a duração desse período é de 1 a 4 dias. No final do período de hipercuidados, a equipe de migração normalmente transfere a responsabilidade pelas aplicações para a equipe de operações de nuvem.

I

IaC

Veja a [infraestrutura como código](#).

Política baseada em identidade

Uma política anexada a um ou mais diretores do IAM que define suas permissões no Nuvem AWS ambiente.

aplicação ociosa

Uma aplicação que tem um uso médio de CPU e memória entre 5 e 20% em um período de 90 dias. Em um projeto de migração, é comum retirar essas aplicações ou retê-las on-premises.

IIoT

Veja a [Internet das Coisas industrial](#).

infraestrutura imutável

Um modelo que implanta uma nova infraestrutura para cargas de trabalho de produção em vez de atualizar, corrigir ou modificar a infraestrutura existente. [Infraestruturas imutáveis são inerentemente mais consistentes, confiáveis e previsíveis do que infraestruturas mutáveis](#). Para obter mais informações, consulte as melhores práticas de [implantação usando infraestrutura imutável](#) no Well-Architected AWS Framework.

VPC de entrada (admissão)

Em uma arquitetura de AWS várias contas, uma VPC que aceita, inspeciona e roteia conexões de rede de fora de um aplicativo. A [Arquitetura de referência de segurança da AWS](#) recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

migração incremental

Uma estratégia de substituição na qual você migra a aplicação em pequenas partes, em vez de realizar uma única substituição completa. Por exemplo, é possível mover inicialmente apenas alguns microsserviços ou usuários para o novo sistema. Depois de verificar se tudo está funcionando corretamente, mova os microsserviços ou usuários adicionais de forma incremental até poder descomissionar seu sistema herdado. Essa estratégia reduz os riscos associados a migrações de grande porte.

Indústria 4.0

Um termo que foi introduzido por [Klaus Schwab](#) em 2016 para se referir à modernização dos processos de fabricação por meio de avanços em conectividade, dados em tempo real, automação, análise e IA/ML.

infraestrutura

Todos os recursos e ativos contidos no ambiente de uma aplicação.

Infraestrutura como código (IaC)

O processo de provisionamento e gerenciamento da infraestrutura de uma aplicação por meio de um conjunto de arquivos de configuração. A IaC foi projetada para ajudar você a centralizar

o gerenciamento da infraestrutura, padronizar recursos e escalar rapidamente para que novos ambientes sejam reproduzíveis, confiáveis e consistentes.

Internet das Coisas Industrial (IIoT)

O uso de sensores e dispositivos conectados à Internet nos setores industriais, como manufatura, energia, automotivo, saúde, ciências biológicas e agricultura. Para obter mais informações, consulte [Construir uma estratégia de transformação digital para a Internet das Coisas Industrial \(IIoT\)](#).

VPC de inspeção

Em uma arquitetura de AWS várias contas, uma VPC centralizada que gerencia as inspeções do tráfego de rede entre VPCs (na mesma ou em diferentes Regiões da AWS), a Internet e as redes locais. A [Arquitetura de referência de segurança da AWS](#) recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

Internet das Coisas (IoT)

A rede de objetos físicos conectados com sensores ou processadores incorporados que se comunicam com outros dispositivos e sistemas pela Internet ou por uma rede de comunicação local. Para obter mais informações, consulte [O que é IoT?](#)

interpretabilidade

Uma característica de um modelo de machine learning que descreve o grau em que um ser humano pode entender como as previsões do modelo dependem de suas entradas. Para obter mais informações, consulte [Interpretabilidade do modelo de machine learning com a AWS](#).

IoT

Consulte [Internet das Coisas](#).

Biblioteca de informações de TI (ITIL)

Um conjunto de práticas recomendadas para fornecer serviços de TI e alinhar esses serviços a requisitos de negócios. A ITIL fornece a base para o ITSM.

Gerenciamento de serviços de TI (ITSM)

Atividades associadas a design, implementação, gerenciamento e suporte de serviços de TI para uma organização. Para obter informações sobre a integração de operações em nuvem com ferramentas de ITSM, consulte o [guia de integração de operações](#).

ITIL

Consulte [a biblioteca de informações](#) de TI.

ITSM

Veja o [gerenciamento de serviços de TI](#).

L

controle de acesso baseado em etiqueta (LBAC)

Uma implementação do controle de acesso obrigatório (MAC) em que os usuários e os dados em si recebem explicitamente um valor de etiqueta de segurança. A interseção entre a etiqueta de segurança do usuário e a etiqueta de segurança dos dados determina quais linhas e colunas podem ser vistas pelo usuário.

zona de pouso

Uma landing zone é um AWS ambiente bem arquitetado, com várias contas, escalável e seguro. Um ponto a partir do qual suas organizações podem iniciar e implantar rapidamente workloads e aplicações com confiança em seu ambiente de segurança e infraestrutura. Para obter mais informações sobre zonas de pouso, consulte [Configurar um ambiente da AWS com várias contas seguro e escalável](#).

migração de grande porte

Uma migração de 300 servidores ou mais.

LBAC

Veja controle de [acesso baseado em etiquetas](#).

privilegio mínimo

A prática recomendada de segurança de conceder as permissões mínimas necessárias para executar uma tarefa. Para obter mais informações, consulte [Aplicar permissões de privilégios mínimos](#) na documentação do IAM.

mover sem alterações (lift-and-shift)

Veja [7 Rs](#).

sistema little-endian

Um sistema que armazena o byte menos significativo antes. Veja também [endianness](#).

ambientes inferiores

Veja o [ambiente](#).

M

machine learning (ML)

Um tipo de inteligência artificial que usa algoritmos e técnicas para reconhecimento e aprendizado de padrões. O ML analisa e aprende com dados gravados, por exemplo, dados da Internet das Coisas (IoT), para gerar um modelo estatístico baseado em padrões. Para obter mais informações, consulte [Machine learning](#).

ramificação principal

Veja a [filial](#).

malware

Software projetado para comprometer a segurança ou a privacidade do computador. O malware pode interromper os sistemas do computador, vaziar informações confidenciais ou obter acesso não autorizado. Exemplos de malware incluem vírus, worms, ransomware, cavalos de Tróia, spyware e keyloggers.

serviços gerenciados

Serviços da AWS para o qual AWS opera a camada de infraestrutura, o sistema operacional e as plataformas, e você acessa os endpoints para armazenar e recuperar dados. O Amazon Simple Storage Service (Amazon S3) e o Amazon DynamoDB são exemplos de serviços gerenciados. Eles também são conhecidos como serviços abstratos.

sistema de execução de manufatura (MES)

Um sistema de software para rastrear, monitorar, documentar e controlar processos de produção que convertem matérias-primas em produtos acabados no chão de fábrica.

MAP

Consulte [Migration Acceleration Program](#).

mecanismo

Um processo completo no qual você cria uma ferramenta, impulsiona a adoção da ferramenta e, em seguida, inspeciona os resultados para fazer ajustes. Um mecanismo é um ciclo que se reforça e se aprimora à medida que opera. Para obter mais informações, consulte [Construindo mecanismos](#) no AWS Well-Architected Framework.

conta-membro

Todos, Contas da AWS exceto a conta de gerenciamento, que fazem parte de uma organização em AWS Organizations. Uma conta só pode ser membro de uma organização de cada vez.

MES

Veja o [sistema de execução de manufatura](#).

Transporte de telemetria de enfileiramento de mensagens (MQTT)

[Um protocolo de comunicação leve machine-to-machine \(M2M\), baseado no padrão de publicação/assinatura, para dispositivos de IoT com recursos limitados.](#)

microserviço

Um serviço pequeno e independente que se comunica por meio de APIs bem definidas e normalmente pertence a equipes pequenas e autônomas. Por exemplo, um sistema de seguradora pode incluir microserviços que mapeiam as capacidades comerciais, como vendas ou marketing, ou subdomínios, como compras, reclamações ou análises. Os benefícios dos microserviços incluem agilidade, escalabilidade flexível, fácil implantação, código reutilizável e resiliência. Para obter mais informações, consulte [Integração de microserviços usando serviços sem AWS servidor](#).

arquitetura de microserviços

Uma abordagem à criação de aplicações com componentes independentes que executam cada processo de aplicação como um microserviço. Esses microserviços se comunicam por meio de uma interface bem definida usando APIs leves. Cada microserviço nessa arquitetura pode ser atualizado, implantado e escalado para atender à demanda por funções específicas de uma aplicação. Para obter mais informações, consulte [Implementação de microserviços em AWS](#)

Programa de Aceleração da Migração (MAP)

Um AWS programa que fornece suporte de consultoria, treinamento e serviços para ajudar as organizações a criar uma base operacional sólida para migrar para a nuvem e ajudar a

compensar o custo inicial das migrações. O MAP inclui uma metodologia de migração para executar migrações legadas de forma metódica e um conjunto de ferramentas para automatizar e acelerar cenários comuns de migração.

migração em escala

O processo de mover a maior parte do portfólio de aplicações para a nuvem em ondas, com mais aplicações sendo movidas em um ritmo mais rápido a cada onda. Essa fase usa as práticas recomendadas e lições aprendidas nas fases anteriores para implementar uma fábrica de migração de equipes, ferramentas e processos para agilizar a migração de workloads por meio de automação e entrega ágeis. Esta é a terceira fase da [estratégia de migração para a AWS](#).

fábrica de migração

Equipes multifuncionais que simplificam a migração de workloads por meio de abordagens automatizadas e ágeis. As equipes da fábrica de migração geralmente incluem operações, analistas e proprietários de negócios, engenheiros de migração, desenvolvedores e DevOps profissionais que trabalham em sprints. Entre 20 e 50% de um portfólio de aplicações corporativas consiste em padrões repetidos que podem ser otimizados por meio de uma abordagem de fábrica. Para obter mais informações, consulte [discussão sobre fábricas de migração](#) e o [guia do Cloud Migration Factory](#) neste conjunto de conteúdo.

metadados de migração

As informações sobre a aplicação e o servidor necessárias para concluir a migração. Cada padrão de migração exige um conjunto de metadados de migração diferente. Exemplos de metadados de migração incluem a sub-rede, o grupo de segurança e AWS a conta de destino.

padrão de migração

Uma tarefa de migração repetível que detalha a estratégia de migração, o destino da migração e a aplicação ou o serviço de migração usado. Exemplo: rehospede a migração para o Amazon EC2 AWS com o Application Migration Service.

Avaliação de Portfólio para Migração (MPA)

Uma ferramenta on-line que fornece informações para validar o caso de negócios para a migração para a AWS nuvem. O MPA fornece avaliação detalhada do portfólio (dimensionamento correto do servidor, preços, comparações de TCO, análise de custos de migração), bem como planejamento de migração (análise e coleta de dados de aplicações, agrupamento de aplicações, priorização de migração e planejamento de ondas). A [ferramenta MPA](#) (requer login) está disponível gratuitamente para todos os AWS consultores e consultores parceiros da APN.

Avaliação de Preparação para Migração (MRA)

O processo de obter insights sobre o status de prontidão de uma organização para a nuvem, identificar pontos fortes e fracos e criar um plano de ação para fechar as lacunas identificadas, usando o CAF. AWS Para mais informações, consulte o [guia de preparação para migração](#). A MRA é a primeira fase da [estratégia de migração para a AWS](#).

estratégia de migração

A abordagem usada para migrar uma carga de trabalho para a AWS nuvem. Para obter mais informações, consulte a entrada de [7 Rs](#) neste glossário e consulte [Mobilize sua organização para acelerar migrações em grande escala](#).

ML

Veja o [aprendizado de máquina](#).

modernização

Transformar uma aplicação desatualizada (herdada ou monolítica) e sua infraestrutura em um sistema ágil, elástico e altamente disponível na nuvem para reduzir custos, ganhar eficiência e aproveitar as inovações. Para obter mais informações, consulte [Estratégia para modernizar aplicativos no Nuvem AWS](#).

avaliação de preparação para modernização

Uma avaliação que ajuda a determinar a preparação para modernização das aplicações de uma organização. Ela identifica benefícios, riscos e dependências e determina o quão bem a organização pode acomodar o estado futuro dessas aplicações. O resultado da avaliação é um esquema da arquitetura de destino, um roteiro que detalha as fases de desenvolvimento e os marcos do processo de modernização e um plano de ação para abordar as lacunas identificadas. Para obter mais informações, consulte [Avaliar a preparação para modernização de aplicações na AWS Cloud](#).

aplicações monolíticas (monólitos)

Aplicações que são executadas como um único serviço com processos fortemente acoplados. As aplicações monolíticas apresentam várias desvantagens. Se um recurso da aplicação apresentar um aumento na demanda, toda a arquitetura deverá ser escalada. Adicionar ou melhorar os recursos de uma aplicação monolítica também se torna mais complexo quando a base de código cresce. Para resolver esses problemas, é possível criar uma arquitetura de microsserviços. Para obter mais informações, consulte [Decompor monólitos em microsserviços](#).

MAPA

Consulte [Avaliação do portfólio de migração](#).

MQTT

Consulte Transporte de [telemetria de enfileiramento de](#) mensagens.

classificação multiclasse

Um processo que ajuda a gerar previsões para várias classes (prevendo um ou mais de dois resultados). Por exemplo, um modelo de ML pode perguntar “Este produto é um livro, um carro ou um telefone?” ou “Qual categoria de produtos é mais interessante para este cliente?”

infraestrutura mutável

Um modelo que atualiza e modifica a infraestrutura existente para cargas de trabalho de produção. Para melhorar a consistência, confiabilidade e previsibilidade, o AWS Well-Architected Framework recomenda o uso de infraestrutura [imutável](#) como uma prática recomendada.

O

OAC

Veja o [controle de acesso de origem](#).

CARVALHO

Veja a [identidade de acesso de origem](#).

OCM

Veja o [gerenciamento de mudanças organizacionais](#).

migração offline

Um método de migração no qual a workload de origem é desativada durante o processo de migração. Esse método envolve tempo de inatividade prolongado e geralmente é usado para workloads pequenas e não críticas.

OI

Veja a [integração de operações](#).

OLA

Veja o [contrato em nível operacional](#).

migração online

Um método de migração no qual a workload de origem é copiada para o sistema de destino sem ser colocada offline. As aplicações conectadas à workload podem continuar funcionando durante a migração. Esse método envolve um tempo de inatividade nulo ou mínimo e normalmente é usado para workloads essenciais para a produção.

OPC-UA

Consulte [Comunicação de processo aberto — Arquitetura unificada](#).

Comunicação de processo aberto — Arquitetura unificada (OPC-UA)

Um protocolo de comunicação machine-to-machine (M2M) para automação industrial. O OPC-UA fornece um padrão de interoperabilidade com esquemas de criptografia, autenticação e autorização de dados.

acordo de nível operacional (OLA)

Um acordo que esclarece o que os grupos funcionais de TI prometem oferecer uns aos outros para apoiar um acordo de serviço (SLA).

análise de prontidão operacional (ORR)

Uma lista de verificação de perguntas e melhores práticas associadas que ajudam você a entender, avaliar, prevenir ou reduzir o escopo de incidentes e possíveis falhas. Para obter mais informações, consulte [Operational Readiness Reviews \(ORR\)](#) no Well-Architected AWS Framework.

tecnologia operacional (OT)

Sistemas de hardware e software que funcionam com o ambiente físico para controlar operações, equipamentos e infraestrutura industriais. Na manufatura, a integração dos sistemas OT e de tecnologia da informação (TI) é o foco principal das transformações [da Indústria 4.0](#).

integração de operações (OI)

O processo de modernização das operações na nuvem, que envolve planejamento de preparação, automação e integração. Para obter mais informações, consulte o [guia de integração de operações](#).

trilha organizacional

Uma trilha criada por ela AWS CloudTrail registra todos os eventos de todos Contas da AWS em uma organização em AWS Organizations. Essa trilha é criada em cada Conta da AWS que faz parte da organização e monitora a atividade em cada conta. Para obter mais informações, consulte [Criação de uma trilha para uma organização](#) na CloudTrail documentação.

gerenciamento de alterações organizacionais (OCM)

Uma estrutura para gerenciar grandes transformações de negócios disruptivas de uma perspectiva de pessoas, cultura e liderança. O OCM ajuda as organizações a se prepararem e fazerem a transição para novos sistemas e estratégias, acelerando a adoção de alterações, abordando questões de transição e promovendo mudanças culturais e organizacionais. Na estratégia de AWS migração, essa estrutura é chamada de aceleração de pessoas, devido à velocidade de mudança necessária nos projetos de adoção da nuvem. Para obter mais informações, consulte o [guia do OCM](#).

controle de acesso de origem (OAC)

Em CloudFront, uma opção aprimorada para restringir o acesso para proteger seu conteúdo do Amazon Simple Storage Service (Amazon S3). O OAC oferece suporte a todos os buckets S3 Regiões da AWS, criptografia do lado do servidor com AWS KMS (SSE-KMS) e solicitações dinâmicas ao bucket S3. PUT DELETE

Identidade do acesso de origem (OAI)

Em CloudFront, uma opção para restringir o acesso para proteger seu conteúdo do Amazon S3. Quando você usa o OAI, CloudFront cria um principal com o qual o Amazon S3 pode se autenticar. Os diretores autenticados podem acessar o conteúdo em um bucket do S3 somente por meio de uma distribuição específica. CloudFront Veja também [OAC](#), que fornece um controle de acesso mais granular e aprimorado.

OU

Veja a [análise de prontidão operacional](#).

NÃO

Veja a [tecnologia operacional](#).

VPC de saída (egresso)

Em uma arquitetura de AWS várias contas, uma VPC que gerencia conexões de rede que são iniciadas de dentro de um aplicativo. A [Arquitetura de referência de segurança da AWS](#)

recomenda configurar sua conta de rede com VPCs de entrada, saída e inspeção para proteger a interface bidirecional entre a aplicação e a Internet em geral.

P

limite de permissões

Uma política de gerenciamento do IAM anexada a entidades principais do IAM para definir as permissões máximas que o usuário ou perfil podem ter. Para obter mais informações, consulte [Limites de permissões](#) na documentação do IAM.

informações de identificação pessoal (PII)

Informações que, quando visualizadas diretamente ou combinadas com outros dados relacionados, podem ser usadas para inferir razoavelmente a identidade de um indivíduo. Exemplos de PII incluem nomes, endereços e informações de contato.

PII

Veja as [informações de identificação pessoal](#).

manual

Um conjunto de etapas predefinidas que capturam o trabalho associado às migrações, como a entrega das principais funções operacionais na nuvem. Um manual pode assumir a forma de scripts, runbooks automatizados ou um resumo dos processos ou etapas necessários para operar seu ambiente modernizado.

PLC

Consulte [controlador lógico programável](#).

AMEIXA

Veja o gerenciamento [do ciclo de vida do produto](#).

política

Um objeto que pode definir permissões (consulte a [política baseada em identidade](#)), especificar as condições de acesso (consulte a [política baseada em recursos](#)) ou definir as permissões máximas para todas as contas em uma organização em AWS Organizations (consulte a política de controle de [serviços](#)).

persistência poliglota

Escolher de forma independente a tecnologia de armazenamento de dados de um microserviço com base em padrões de acesso a dados e outros requisitos. Se seus microserviços tiverem a mesma tecnologia de armazenamento de dados, eles poderão enfrentar desafios de implementação ou apresentar baixa performance. Os microserviços serão implementados com mais facilidade e alcançarão performance e escalabilidade melhores se usarem o armazenamento de dados mais bem adaptado às suas necessidades. Para obter mais informações, consulte [Habilitar a persistência de dados em microserviços](#).

avaliação do portfólio

Um processo de descobrir, analisar e priorizar o portfólio de aplicações para planejar a migração. Para obter mais informações, consulte [Avaliar a preparação para a migração](#).

predicado

Uma condição de consulta que retorna `true` ou `false`, normalmente localizada em uma `WHERE` cláusula.

pressão de predicados

Uma técnica de otimização de consulta de banco de dados que filtra os dados na consulta antes da transferência. Isso reduz a quantidade de dados que devem ser recuperados e processados do banco de dados relacional e melhora o desempenho das consultas.

controle preventivo

Um controle de segurança projetado para evitar que um evento ocorra. Esses controles são a primeira linha de defesa para ajudar a evitar acesso não autorizado ou alterações indesejadas em sua rede. Para obter mais informações, consulte [Controles preventivos](#) em Como implementar controles de segurança na AWS.

principal (entidade principal)

Uma entidade AWS que pode realizar ações e acessar recursos. Essa entidade geralmente é um usuário raiz para um Conta da AWS, uma função do IAM ou um usuário. Para obter mais informações, consulte Entidade principal em [Termos e conceitos de perfis](#) na documentação do IAM.

Privacidade por design

Uma abordagem em engenharia de sistemas que leva em consideração a privacidade em todo o processo de engenharia.

zonas hospedadas privadas

Um contêiner que armazena informações sobre como você quer que o Amazon Route 53 responda a consultas ao DNS para um domínio e seus subdomínios dentro de uma ou mais VPCs. Para obter mais informações, consulte [Como trabalhar com zonas hospedadas privadas](#) na documentação do Route 53.

controle proativo

Um [controle de segurança](#) projetado para impedir a implantação de recursos não compatíveis. Esses controles examinam os recursos antes de serem provisionados. Se o recurso não estiver em conformidade com o controle, ele não será provisionado. Para obter mais informações, consulte o [guia de referência de controles](#) na AWS Control Tower documentação e consulte [Controles proativos](#) em Implementação de controles de segurança em AWS.

gerenciamento do ciclo de vida do produto (PLM)

O gerenciamento de dados e processos de um produto em todo o seu ciclo de vida, desde o design, desenvolvimento e lançamento, passando pelo crescimento e maturidade, até o declínio e a remoção.

ambiente de produção

Veja o [ambiente](#).

controlador lógico programável (PLC)

Na fabricação, um computador altamente confiável e adaptável que monitora as máquinas e automatiza os processos de fabricação.

pseudonimização

O processo de substituir identificadores pessoais em um conjunto de dados por valores de espaço reservado. A pseudonimização pode ajudar a proteger a privacidade pessoal. Os dados pseudonimizados ainda são considerados dados pessoais.

publicar/assinar (pub/sub)

Um padrão que permite comunicações assíncronas entre microsserviços para melhorar a escalabilidade e a capacidade de resposta. Por exemplo, em um [MES](#) baseado em microsserviços, um microsserviço pode publicar mensagens de eventos em um canal no qual outros microsserviços possam se inscrever. O sistema pode adicionar novos microsserviços sem alterar o serviço de publicação.

Q

plano de consulta

Uma série de etapas, como instruções, usadas para acessar os dados em um sistema de banco de dados relacional SQL.

regressão de planos de consultas

Quando um otimizador de serviço de banco de dados escolhe um plano menos adequado do que escolhia antes de uma determinada alteração no ambiente de banco de dados ocorrer. Isso pode ser causado por alterações em estatísticas, restrições, configurações do ambiente, associações de parâmetros de consulta e atualizações do mecanismo de banco de dados.

R

Matriz RACI

Veja [responsável, responsável, consultado, informado \(RACI\)](#).

ransomware

Um software mal-intencionado desenvolvido para bloquear o acesso a um sistema ou dados de computador até que um pagamento seja feito.

Matriz RASCI

Veja [responsável, responsável, consultado, informado \(RACI\)](#).

RCAC

Veja o [controle de acesso por linha e coluna](#).

réplica de leitura

Uma cópia de um banco de dados usada somente para leitura. É possível encaminhar consultas para a réplica de leitura e reduzir a carga no banco de dados principal.

rearquiteta

Veja [7 Rs](#).

objetivo de ponto de recuperação (RPO)

Período de tempo aceitável máximo desde o último ponto de recuperação de dados. Determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

objetivo de tempo de recuperação (RTO)

O atraso máximo aceitável entre a interrupção e a restauração do serviço.

refatorar

Veja [7 Rs](#).

Região

Uma coleção de AWS recursos em uma área geográfica. Cada um Região da AWS é isolado e independente dos outros para fornecer tolerância a falhas, estabilidade e resiliência. Para obter mais informações, consulte [Especificar o que Regiões da AWS sua conta pode usar](#).

regressão

Uma técnica de ML que prevê um valor numérico. Por exemplo, para resolver o problema de “Por qual preço esta casa será vendida?” um modelo de ML pode usar um modelo de regressão linear para prever o preço de venda de uma casa com base em fatos conhecidos sobre a casa (por exemplo, a metragem quadrada).

redefinir a hospedagem

Veja [7 Rs](#).

versão

Em um processo de implantação, o ato de promover mudanças em um ambiente de produção.

realocar

Veja [7 Rs](#).

redefinir a plataforma

Veja [7 Rs](#).

recomprar

Veja [7 Rs](#).

resiliência

A capacidade de um aplicativo de resistir ou se recuperar de interrupções. [Alta disponibilidade](#) e [recuperação de desastres](#) são considerações comuns ao planejar a resiliência no. Nuvem AWS. Para obter mais informações, consulte [Nuvem AWS Resiliência](#).

política baseada em recurso

Uma política associada a um recurso, como um bucket do Amazon S3, um endpoint ou uma chave de criptografia. Esse tipo de política especifica quais entidades principais têm acesso permitido, ações válidas e quaisquer outras condições que devem ser atendidas.

matriz responsável, accountable, consultada, informada (RACI)

Uma matriz que define as funções e responsabilidades de todas as partes envolvidas nas atividades de migração e nas operações de nuvem. O nome da matriz é derivado dos tipos de responsabilidade definidos na matriz: responsável (R), responsabilizável (A), consultado (C) e informado (I). O tipo de suporte (S) é opcional. Se você incluir suporte, a matriz será chamada de matriz RASCI e, se excluir, será chamada de matriz RACI.

controle responsivo

Um controle de segurança desenvolvido para conduzir a remediação de eventos adversos ou desvios em relação à linha de base de segurança. Para obter mais informações, consulte [Controles responsivos](#) em Como implementar controles de segurança na AWS.

reter

Veja [7 Rs](#).

aposentar-se

Veja [7 Rs](#).

rotação

O processo de atualizar periodicamente um [segredo](#) para dificultar o acesso das credenciais por um invasor.

controle de acesso por linha e coluna (RCAC)

O uso de expressões SQL básicas e flexíveis que tenham regras de acesso definidas. O RCAC consiste em permissões de linha e máscaras de coluna.

RPO

Veja o [objetivo do ponto de recuperação](#).

RTO

Veja o [objetivo do tempo de recuperação](#).

runbook

Um conjunto de procedimentos manuais ou automatizados necessários para realizar uma tarefa específica. Eles são normalmente criados para agilizar operações ou procedimentos repetitivos com altas taxas de erro.

S

SAML 2.0

Um padrão aberto que muitos provedores de identidade (IdPs) usam. Esse recurso permite o login único federado (SSO), para que os usuários possam fazer login AWS Management Console ou chamar as operações da AWS API sem que você precise criar um usuário no IAM para todos em sua organização. Para obter mais informações sobre a federação baseada em SAML 2.0, consulte [Sobre a federação baseada em SAML 2.0](#) na documentação do IAM.

SCADA

Veja [controle de supervisão e aquisição de dados](#).

SCP

Veja a [política de controle de serviços](#).

secret

Em AWS Secrets Manager, informações confidenciais ou restritas, como uma senha ou credenciais de usuário, que você armazena de forma criptografada. Ele consiste no valor secreto e em seus metadados. O valor secreto pode ser binário, uma única string ou várias strings. Para obter mais informações, consulte [Secret](#) na documentação do Secrets Manager.

controle de segurança

Uma barreira de proteção técnica ou administrativa que impede, detecta ou reduz a capacidade de uma ameaça explorar uma vulnerabilidade de segurança. [Existem quatro tipos principais de controles de segurança: preventivos, detectivos, responsivos e proativos.](#)

fortalecimento da segurança

O processo de reduzir a superfície de ataque para torná-la mais resistente a ataques. Isso pode incluir ações como remover recursos que não são mais necessários, implementar a prática recomendada de segurança de conceder privilégios mínimos ou desativar recursos desnecessários em arquivos de configuração.

sistema de gerenciamento de eventos e informações de segurança (SIEM)

Ferramentas e serviços que combinam sistemas de gerenciamento de informações de segurança (SIM) e gerenciamento de eventos de segurança (SEM). Um sistema SIEM coleta, monitora e analisa dados de servidores, redes, dispositivos e outras fontes para detectar ameaças e violações de segurança e gerar alertas.

automação de resposta de segurança

Uma ação predefinida e programada projetada para responder ou remediar automaticamente um evento de segurança. Essas automações servem como controles de segurança [responsivos](#) ou [detectivos](#) que ajudam você a implementar as melhores práticas AWS de segurança. Exemplos de ações de resposta automatizada incluem a modificação de um grupo de segurança da VPC, a correção de uma instância do Amazon EC2 ou a rotação de credenciais.

Criptografia do lado do servidor

Criptografia dos dados em seu destino, por AWS service (Serviço da AWS) quem os recebe.

política de controle de serviços (SCP)

Uma política que fornece controle centralizado sobre as permissões de todas as contas em uma organização no AWS Organizations. As SCPs definem barreiras de proteção ou estabelecem limites para as ações que um administrador pode delegar a usuários ou perfis. É possível usar SCPs como listas de permissão ou de negação para especificar quais serviços ou ações são permitidos ou proibidos. Para obter mais informações, consulte [Políticas de controle de serviço](#) na AWS Organizations documentação.

service endpoint (endpoint de serviço)

O URL do ponto de entrada para um AWS service (Serviço da AWS). Você pode usar o endpoint para se conectar programaticamente ao serviço de destino. Para obter mais informações, consulte [Endpoints do AWS service \(Serviço da AWS\)](#) na Referência geral da AWS.

acordo de serviço (SLA)

Um acordo que esclarece o que uma equipe de TI promete fornecer aos clientes, como tempo de atividade e performance do serviço.

indicador de nível de serviço (SLI)

Uma medida de um aspecto de desempenho de um serviço, como taxa de erro, disponibilidade ou taxa de transferência.

objetivo de nível de serviço (SLO)

Uma métrica alvo que representa a integridade de um serviço, conforme medida por um indicador de [nível de serviço](#).

modelo de responsabilidade compartilhada

Um modelo que descreve a responsabilidade com a qual você compartilha AWS pela segurança e conformidade na nuvem. AWS é responsável pela segurança da nuvem, enquanto você é responsável pela segurança na nuvem. Para obter mais informações, consulte o [Modelo de responsabilidade compartilhada](#).

SIEM

Veja [informações de segurança e sistema de gerenciamento de eventos](#).

ponto único de falha (SPOF)

Uma falha em um único componente crítico de um aplicativo que pode interromper o sistema.

SLA

Veja o contrato [de nível de serviço](#).

ESGUIO

Veja o indicador [de nível de serviço](#).

SLO

Veja o objetivo do [nível de serviço](#).

split-and-seed modelo

Um padrão para escalar e acelerar projetos de modernização. À medida que novos recursos e lançamentos de produtos são definidos, a equipe principal se divide para criar novas equipes

de produtos. Isso ajuda a escalar os recursos e os serviços da sua organização, melhora a produtividade do desenvolvedor e possibilita inovações rápidas. Para obter mais informações, consulte [Abordagem em fases para modernizar aplicativos no](#). Nuvem AWS

CUSPE

Veja [um único ponto de falha](#).

esquema de estrelas

Uma estrutura organizacional de banco de dados que usa uma grande tabela de fatos para armazenar dados transacionais ou medidos e usa uma ou mais tabelas dimensionais menores para armazenar atributos de dados. Essa estrutura foi projetada para uso em um [data warehouse](#) ou para fins de inteligência comercial.

padrão strangler fig

Uma abordagem à modernização de sistemas monolíticos que consiste em reescrever e substituir incrementalmente a funcionalidade do sistema até que o sistema herdado possa ser desativado. Esse padrão usa a analogia de uma videira que cresce e se torna uma árvore estabelecida e, eventualmente, supera e substitui sua hospedeira. O padrão foi [apresentado por Martin Fowler](#) como forma de gerenciar riscos ao reescrever sistemas monolíticos. Para ver um exemplo de como aplicar esse padrão, consulte [Modernizar incrementalmente os serviços Web herdados do Microsoft ASP.NET \(ASMX\) usando contêineres e o Amazon API Gateway](#).

sub-rede

Um intervalo de endereços IP na VPC. Uma sub-rede deve residir em uma única zona de disponibilidade.

controle de supervisão e aquisição de dados (SCADA)

Na manufatura, um sistema que usa hardware e software para monitorar ativos físicos e operações de produção.

symmetric encryption (criptografia simétrica)

Um algoritmo de criptografia que usa a mesma chave para criptografar e descriptografar dados.

testes sintéticos

Testar um sistema de forma que simule as interações do usuário para detectar possíveis problemas ou monitorar o desempenho. Você pode usar o [Amazon CloudWatch Synthetics](#) para criar esses testes.

T

tags

Pares de valores-chave que atuam como metadados para organizar seus recursos. AWS As tags podem ajudar você a gerenciar, identificar, organizar, pesquisar e filtrar recursos. Para obter mais informações, consulte [Marcar seus recursos do AWS](#).

variável-alvo

O valor que você está tentando prever no ML supervisionado. Ela também é conhecida como variável de resultado. Por exemplo, em uma configuração de fabricação, a variável-alvo pode ser um defeito do produto.

lista de tarefas

Uma ferramenta usada para monitorar o progresso por meio de um runbook. Uma lista de tarefas contém uma visão geral do runbook e uma lista de tarefas gerais a serem concluídas. Para cada tarefa geral, ela inclui o tempo estimado necessário, o proprietário e o progresso.

ambiente de teste

Veja o [ambiente](#).

treinamento

O processo de fornecer dados para que seu modelo de ML aprenda. Os dados de treinamento devem conter a resposta correta. O algoritmo de aprendizado descobre padrões nos dados de treinamento que mapeiam os atributos dos dados de entrada no destino (a resposta que você deseja prever). Ele gera um modelo de ML que captura esses padrões. Você pode usar o modelo de ML para obter previsões de novos dados cujo destino você não conhece.

gateway de trânsito

Um hub de trânsito de rede que pode ser usado para interconectar as VPCs e as redes on-premises. Para obter mais informações, consulte [O que é um gateway de trânsito](#) na AWS Transit Gateway documentação.

fluxo de trabalho baseado em troncos

Uma abordagem na qual os desenvolvedores criam e testam recursos localmente em uma ramificação de recursos e, em seguida, mesclam essas alterações na ramificação principal. A

ramificação principal é então criada para os ambientes de desenvolvimento, pré-produção e produção, sequencialmente.

Acesso confiável

Conceder permissões a um serviço que você especifica para realizar tarefas em sua organização AWS Organizations e em suas contas em seu nome. O serviço confiável cria um perfil vinculado ao serviço em cada conta, quando esse perfil é necessário, para realizar tarefas de gerenciamento para você. Para obter mais informações, consulte [Usando AWS Organizations com outros AWS serviços](#) na AWS Organizations documentação.

tuning (ajustar)

Alterar aspectos do processo de treinamento para melhorar a precisão do modelo de ML. Por exemplo, você pode treinar o modelo de ML gerando um conjunto de rótulos, adicionando rótulos e repetindo essas etapas várias vezes em configurações diferentes para otimizar o modelo.

equipe de duas pizzas

Uma pequena DevOps equipe que você pode alimentar com duas pizzas. Uma equipe de duas pizzas garante a melhor oportunidade possível de colaboração no desenvolvimento de software.

U

incerteza

Um conceito que se refere a informações imprecisas, incompletas ou desconhecidas que podem minar a confiabilidade dos modelos preditivos de ML. Há dois tipos de incertezas: a incerteza epistêmica é causada por dados limitados e incompletos, enquanto a incerteza aleatória é causada pelo ruído e pela aleatoriedade inerentes aos dados. Para obter mais informações, consulte o guia [Como quantificar a incerteza em sistemas de aprendizado profundo](#).

tarefas indiferenciadas

Também conhecido como trabalho pesado, trabalho necessário para criar e operar um aplicativo, mas que não fornece valor direto ao usuário final nem oferece vantagem competitiva. Exemplos de tarefas indiferenciadas incluem aquisição, manutenção e planejamento de capacidade.

ambientes superiores

Veja o [ambiente](#).

V

aspiração

Uma operação de manutenção de banco de dados que envolve limpeza após atualizações incrementais para recuperar armazenamento e melhorar a performance.

controle de versões

Processos e ferramentas que rastreiam mudanças, como alterações no código-fonte em um repositório.

emparelhamento de VPC

Uma conexão entre duas VPCs que permite rotear tráfego usando endereços IP privados. Para ter mais informações, consulte [O que é emparelhamento de VPC?](#) na documentação da Amazon VPC.

vulnerabilidade

Uma falha de software ou hardware que compromete a segurança do sistema.

W

cache quente

Um cache de buffer que contém dados atuais e relevantes que são acessados com frequência. A instância do banco de dados pode ler do cache do buffer, o que é mais rápido do que ler da memória principal ou do disco.

dados mornos

Dados acessados raramente. Ao consultar esse tipo de dados, consultas moderadamente lentas geralmente são aceitáveis.

função de janela

Uma função SQL que executa um cálculo em um grupo de linhas que se relacionam de alguma forma com o registro atual. As funções de janela são úteis para processar tarefas, como calcular uma média móvel ou acessar o valor das linhas com base na posição relativa da linha atual.

workload

Uma coleção de códigos e recursos que geram valor empresarial, como uma aplicação voltada para o cliente ou um processo de back-end.

workstreams

Grupos funcionais em um projeto de migração que são responsáveis por um conjunto específico de tarefas. Cada workstream é independente, mas oferece suporte aos outros workstreams do projeto. Por exemplo, o workstream de portfólio é responsável por priorizar aplicações, planejar ondas e coletar metadados de migração. O workstream de portfólio entrega esses ativos ao workstream de migração, que então migra os servidores e as aplicações.

MINHOCA

Veja [escrever uma vez, ler muitas](#).

WQF

Consulte o [AWS Workload Qualification Framework](#).

escreva uma vez, leia muitas (WORM)

Um modelo de armazenamento que grava dados uma única vez e evita que os dados sejam excluídos ou modificados. Os usuários autorizados podem ler os dados quantas vezes forem necessárias, mas não podem alterá-los. Essa infraestrutura de armazenamento de dados é considerada [imutável](#).

Z

exploração de dia zero

Um ataque, geralmente malware, que tira proveito de uma vulnerabilidade de [dia zero](#).

vulnerabilidade de dia zero

Uma falha ou vulnerabilidade não mitigada em um sistema de produção. Os agentes de ameaças podem usar esse tipo de vulnerabilidade para atacar o sistema. Os desenvolvedores frequentemente ficam cientes da vulnerabilidade como resultado do ataque.

aplicação zumbi

Uma aplicação que tem um uso médio de CPU e memória inferior a 5%. Em um projeto de migração, é comum retirar essas aplicações.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.