Tools und bewährte Methoden zur Überwachung und Warnung für Amazon RDS for MySQL und MariaDB

# AWS Präskriptive Leitlinien

# AWS Präskriptive Leitlinien: Tools und bewährte Methoden zur Überwachung und Warnung für Amazon RDS for MySQL und MariaDB

# Table of Contents

# Überwachungs- und Warnungstools und bewährte Methoden für Amazon RDS für MySQL und MariaDB

Igor Obradovic, Amazon Web Services (AWS)

Juni 2023(Verlauf dokumentieren)

Datenbanküberwachung ist der Prozess der Messung, Verfolgung und Bewertung der Verfügbarkeit, Leistung und Funktionalität einer Datenbank. Überwachungs- und Warnlösungen helfen Unternehmen dabei, sicherzustellen, dass ihre Datenbankdienste und damit die zugehörigen Anwendungen und Workloads sicher, leistungsstark, robust und effizient sind. In AWS können Sie Ihre Workload-Logs, Metriken, Ereignisse und Traces sammeln und analysieren, um den Zustand Ihres Workloads zu verstehen und Erkenntnisse aus den Betriebsabläufen im Laufe der Zeit zu gewinnen.

Sie können Ihre Ressourcen überwachen, um sicherzustellen, dass sie wie erwartet funktionieren, und um Probleme zu erkennen und zu beheben, bevor sie sich auf Ihre Kunden auswirken. Sie sollten die von Ihnen überwachten Metriken, Protokolle, Ereignisse und Traces verwenden, um bei Überschreitung von Schwellenwerten Alarme auszulösen.

In diesem Handbuch werden Tools zur Datenbankbeobachtbarkeit und -überwachung sowie bewährte Methoden für Amazon Relational Database Service (Amazon RDS) -Datenbanken beschrieben. Der Leitfaden konzentriert sich auf MySQL- und MariaDB-Datenbanken, obwohl die meisten Informationen auch für andere Amazon RDS-Datenbank-Engines gelten.

Dieser Leitfaden richtet sich an Lösungsarchitekten, Datenbankarchitekten, DBAs und SeniorDevOpsTechniker und andere Teammitglieder, die sich mit der Entwicklung, Implementierung und Verwaltung von Überwachungs- und Observabilitätslösungen für ihre in der AWS-Cloud laufenden Datenbank-Workloads befassen.

Inhalt

# Übersicht

Überwachung und Warnung sind in vier Säulen des AWS Well-Architected Framework enthalten.

- Die Säule der Operational Excellence, dass Ihr Workload so konzipiert sein sollte, dass er Telemetrie und Überwachung umfasst. - AWS Services wie Amazon Relational Database Service (Amazon RDS) stellen die Informationen bereit, die Sie benötigen, um den internen Status Ihres Workloads zu verstehen (z. B. Metriken, Protokolle, Ereignisse und Ablaufverfolgungen). Wenn Sie Ihre Amazon-RDS-Datenbanken betreiben, möchten Sie den Zustand Ihrer Datenbank-Instances verstehen, Betriebsereignisse erkennen und sowohl auf geplante als auch auf ungeplante Ereignisse reagieren können. AWS bietet Überwachungstools, mit denen Sie feststellen können, wann die Unternehmens- und Geschäftsergebnisse gefährdet sind oder potenziell gefährdet sein könnten, sodass Sie zum richtigen Zeitpunkt die entsprechenden Maßnahmen ergreifen können.
- Die Säule der Leistungseffizienz, die Sie bei der Überwachung der Leistung Ihrer Ressourcen wie Amazon-RDS-DB-Instances berücksichtigen sollten, indem Sie leistungsbezogene Metriken in Echtzeit erfassen, aggregieren und verarbeiten. Sie können Leistungseinbußen identifizieren und die Faktoren beheben, z. B. nicht optimierte SQL-Abfragen oder unzureichende Konfigurationsparameter, die dies verursacht haben. Sie können Alarme automatisch auslösen, wenn die Messungen außerhalb der erwarteten Grenzen liegen. Wir empfehlen, dass Sie Alarme nicht nur für Benachrichtigungen verwenden, sondern auch für automatisierte Aktionen als Reaktion auf die erkannten Ereignisse. Sie können die Metriken, die Sie sammeln, anhand vordefinierter Schwellenwerte bewerten oder Machine-Learning-Algorithmen verwenden, um ungewöhnliches Verhalten zu identifizieren. Um beispielsweise einen Trend einer erhöhten CPU-Auslastung zu erkennen, können Sie die `cpuUtilization.total` Metrik über einen bestimmten Zeitraum erfassen und analysieren. Warnungen zu dieser Anomalie können Ihnen proaktiv helfen, das Problem zu beheben, bevor es sich auf Ihre Kunden auswirkt, bevor die CPU-Auslastung das harte Limit erreicht.
- Die Säule der Zuverlässigkeit definiert Überwachung und Warnungen als entscheidend, um sicherzustellen, dass Sie Ihre Verfügbarkeitsanforderungen erfüllen. Ihre Überwachungslösung muss in der Lage sein, Fehler effektiv zu erkennen. Wenn es Probleme oder Ausfälle erkennt, besteht sein Hauptziel darin, bei diesen Problemen zu warnen. Die Implementierung kontinuierlicher Beobachtbarkeits- und Überwachungsmethoden ist für ausfallsichere Architekturen in der Cloud unerlässlich. Um Ihre Workloads zu verbessern, müssen Sie in der Lage sein, sie zu messen und ihren Zustand und Zustand zu verstehen. Die Gestaltungsprinzipien für die

automatische Wiederherstellung nach einem Ausfall, die horizontale Skalierbarkeit und die Kapazitätsbereitstellung hängen von genauen Überwachungs- und Warnservices ab.

- Die Säule der Sicherheit befasst sich mit der Erkennung und Verhinderung unerwarteter oder unerwünschter Konfigurationsänderungen und unerwartetem Verhalten. Sie können Ihre DB-Instances von Amazon RDS für MySQL und MariaDB mit dem MariaDB-Audit-Plugin konfigurieren, um Datenbankaktivitäten wie Benutzeranmeldungen und spezifische Operationen aufzuzeichnen, die für die Datenbank ausgeführt werden. Das Plugin speichert den Datensatz der Datenbankaktivitäten in einer Protokolldatei, die in Überwachungs- und Warntools integriert und importiert werden kann. Die Protokolldatei wird in Echtzeit auf unerwartetes oder verdächtiges Verhalten in Ihrer Datenbank analysiert. Ein solches unerwartetes oder verdächtiges Verhalten kann darauf hinweisen, dass Ihre Amazon-RDS-DB-Instance kompromittiert wurde, was auf potenzielle Risiken für Ihr Unternehmen hinweist. Wenn das Überwachungstool ein solches Ereignis erkennt, wird ein Alarm ausgelöst, um eine Reaktion auf den Sicherheitsvorfall auszulösen, der dazu beiträgt, verdächtige und böswillige Aktivitäten zu beheben.

## Gezielte Geschäftsergebnisse

Durch die Implementierung bewährter Methoden für Überwachungs- und Warnmechanismen können Sie eine leistungsstarke, belastbare, effiziente, sichere und kostenoptimierte Infrastruktur für Ihre Anwendungen und Workloads sicherstellen. Sie können Beobachtbarkeitstools verwenden, die Metriken, Ereignisse, Ablaufverfolgungen und Protokolle in Echtzeit erfassen, speichern und visualisieren, um das Gesamtbild des Zustands und der Leistung Ihrer Datenbanken zu beobachten und zu analysieren und so die Beeinträchtigung oder Unterbrechung Ihrer zugehörigen IT-Services zu verhindern. Wenn es immer noch zu einer ungeplanten Beeinträchtigung oder Serviceunterbrechung kommt, helfen Ihnen Überwachungs- und Warntools bei der rechtzeitigen Erkennung des Problems, der Eskalation, der Reaktion sowie der schnellen Untersuchung und Lösung. Eine umfassende Überwachungs- und Warnlösung für Ihre Cloud-Datenbank-Workloads hilft Ihnen, die folgenden Geschäftsergebnisse zu erzielen:

- Verbessern Sie das Kundenerlebnis. Zuverlässiger Service verbessert das Erlebnis Ihrer Kunden. Datenbanken sind oft eine wichtige Komponente digitaler Services wie Web- und mobile Anwendungen, Medien-Streaming, Zahlungen, business-to-business (B2B)-APIs und Integrationsservices. Wenn Sie Warnmeldungen in Ihren Datenbanken überwachen und einrichten können, um Probleme schnell zu erkennen, effizient zu untersuchen und sie so schnell wie möglich zu beheben, um Ausfallzeiten und andere Unterbrechungen zu minimieren, können Sie die Verfügbarkeit, Sicherheit und Leistung des digitalen Services für Ihre Kunden verbessern.

- Kundenvertrauen aufbauen. Eine bessere Leistung und ein reibungsloseres Benutzererlebnis helfen Ihnen dabei, das Vertrauen Ihrer Kunden zu gewinnen, was zu mehr Geschäft auf Ihrer Plattform führen kann. Beispielsweise kann ein Zahlungsverarbeitungsdienstanbieter, der einen zuverlässigen Online-Service anbietet, ein hohes Kundenvertrauen und eine hohe Kundenbindung erwarten, was zu mehr Kunden und besserer Kundenbindung, einem Anstieg abrechenbarer Transaktionen und neuen, innovativen Services führt, die zu mehr Umsatz führen.
- Vermeiden Sie finanzielle Verluste. Jede unerwartete Ausfallzeit in Ihrer Datenbankinfrastruktur kann sich auf die Geschäftstransaktionen auswirken, die Ihre Kunden mithilfe Ihrer Anwendung ausführen. Dies kann in einigen Fällen zu erheblichen finanziellen Verlusten führen. Verstöße gegen Service Level Agreements (SLAs) können zu einem Verlust des Kundenvertrauens und somit zu einem Umsatzverlust führen. Es kann auch eine rechtliche Grundlage für teure Tests werden, bei denen Kunden möglicherweise eine Anpassung auf der Grundlage Ihrer Haftungs- und Garantievereinbarungen verlangen. Laut einer Untersuchung der Atlassian Corporation, einem Softwareunternehmen, liegen die durchschnittlichen Kosten für Serviceausfälle im Bereich von 140 000 USD pro Stunde, je nach Art und Größe des Unternehmens. Eine stabile Datenbankumgebung ist der Schlüssel zur Vermeidung langer Ausfälle und Geschäftsverluste.
- Erweitern Sie den Wert. Überwachungs- und Warnungsmechanismen können Ihnen helfen, einen hochverfügbaren, belastbaren, zuverlässigen, leistungsfähigen, kosteneffektiven und sicheren digitalen Service zu entwerfen, zu entwickeln und zu betreiben, aber es ist nur der Anfang. Sie möchten, dass Ihre Organisation im Laufe der Zeit skaliert und optimiert wird, bestehende Cloud-Workloads verbessert und neue Services einführt. Neue Services bieten Ihren Kunden zusätzlichen Nutzen und mehr Umsatz für Ihr Unternehmen, was sich auf das Wachstum Ihres Unternehmens auswirkt.
- Verbessern Sie die Produktivität der Entwickler. Entwickler, die produktiv und effizient sind und bei ihren Entwicklungsaufgaben keine Probleme und Engpässe haben, können in kürzerer Zeit hochwertige Produkte bereitstellen. Softwareentwicklung und IT-Betrieb stellen jedoch häufig komplexe Herausforderungen dar, und diese Komplexität steigt mit der Größe der Workloads und ihrer Architekturen. Um Leistung und Konsistenz über verteilte Anwendungen hinweg zu analysieren, benötigen Entwickler Tools, die korrelierte Metriken und Ablaufverfolgungen bereitstellen können. Diese helfen dabei, Artefakte und Infrastrukturkomponenten von Hängecode so schnell wie möglich zu identifizieren und die Auswirkungen auf Endbenutzer zu ermitteln. Die richtige Suite von Tools zur Überwachung und Warnung kann Entwicklern dabei helfen, besser und schneller Code und Tests durchzuführen.
- Verbessern Sie die betriebliche Effektivität und Effizienz. Wenn Sie Cloud-Workloads in großem Umfang betreiben, kann selbst ein kleiner Prozentsatz der Leistungsverbesserungen

zu Einsparungen in Millionen von Dollar führen. Durch die Überwachung Ihrer Datenbanken und die Analyse von Metriken, Ereignissen, Protokollen und Ablaufverfolgungen können Sie Ihre zukünftigen Kapazitätsanforderungen verstehen und vorhersagen und die in der AWS Cloud verfügbaren Kosteneinsparungen nutzen. Wenn Sie Ihre Amazon-RDS-Workloads und den Betriebszustand verstehen, können Sie auf Ereignisse reagieren, Probleme beheben und Verbesserungen planen.

# Allgemeine bewährte Verfahren

Die folgenden bewährten Methoden helfen Ihnen dabei, einen ausreichenden Überblick über den Zustand Ihres Amazon RDS-Workloads zu erhalten und geeignete Maßnahmen als Reaktion auf betriebliche Ereignisse und Überwachungsdaten zu ergreifen.

- Identifizieren Sie KPIs.Identifizieren Sie wichtige Leistungsindikatoren (KPIs) auf der Grundlage der gewünschten Geschäftsergebnisse. Bewerten Sie KPIs, um den Workload-Erfolg zu ermitteln. Wenn Ihr Kerngeschäft beispielsweise E-Commerce ist, könnte eines Ihrer gewünschten Geschäftsergebnisse darin bestehen, dass Ihr E-Shop Ihren Kunden rund um die Uhr für Einkäufe zur Verfügung steht. Um dieses Geschäftsergebnis zu erzielen, definieren Sie den Verfügbarkeits-KPI für die Amazon RDS-Datenbank im Backend, die Ihre E-Shop-Anwendung verwendet, und legen den Basis-KPI wöchentlich auf 99,99% fest. Wenn Sie den tatsächlichen Verfügbarkeits-KPI anhand des Basiswerts auswerten, können Sie feststellen, ob Sie die gewünschte Datenbankverfügbarkeit von 99,99% erreichen und somit das Geschäftsergebnis eines 24/7-Service erzielen.
- Definieren Sie Workload-Metriken.Definieren Sie Workload-Metriken, um die Menge und Qualität Ihres Amazon RDS-Workloads zu messen. Bewerten Sie Kennzahlen, um festzustellen, ob der Workload die gewünschten Ergebnisse erzielt, und um den Zustand des Workloads zu ermitteln. Um beispielsweise den Verfügbarkeits-KPI für Ihre Amazon RDS-DB-Instance zu bewerten, sollten Sie Kennzahlen wie Verfügbarkeit und Ausfallzeit für die DB-Instance messen. Sie können diese Metriken dann verwenden, um den Verfügbarkeits-KPI wie folgt zu berechnen:

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

  Metriken stellen zeitlich geordnete Sätze von Datenpunkten dar. Metriken können auch Dimensionen enthalten, die bei der Kategorisierung und Analyse nützlich sind.
- Erfassen und analysieren Sie Workload-Metriken.Amazon RDS generiert je nach Konfiguration unterschiedliche Metriken und Protokolle. Einige davon stehen für DB-Instance-Ereignisse, Zähler oder Statistiken wie`db.Cache.innoDB_buffer_pool_hits`. Andere Metriken stammen aus dem Betriebssystem, wie`memory.Total`, das die Gesamtspeichermenge der Host-Instance von Amazon Elastic Compute Cloud (Amazon EC2) misst. Das Überwachungstool sollte regelmäßige, proaktive Analysen der gesammelten Kennzahlen durchführen, um Trends zu erkennen und festzustellen, ob geeignete Maßnahmen erforderlich sind.

- Legen Sie Basiswerte für Workload-Metriken fest.Legen Sie Basiswerte für Kennzahlen fest, um erwartete Werte zu definieren und gute oder schlechte Schwellenwerte zu identifizieren. Sie könnten zum Beispiel den Basisplan definieren für`ReadIOPSum` bei normalem Datenbankoperationen bis zu 1.000 zu betragen. Sie können diesen Ausgangswert dann zum Vergleich und zur Identifizierung einer Überauslastung verwenden. Wenn Ihre neuen Kennzahlen durchweg zeigen, dass die Lese-IOPS im Bereich von 2.000 bis 3.000 liegen, haben Sie eine Abweichung identifiziert, die eine Reaktion zur Untersuchung, Intervention und Verbesserung auslösen könnte.
- Informieren Sie sich, wenn die Ergebnisse der Arbeitslast gefährdet sind.Wenn Sie feststellen, dass das Geschäftsergebnis gefährdet ist, geben Sie eine Warnung aus. Sie können dann entweder proaktiv Probleme lösen, bevor sie sich auf Ihre Kunden auswirken, oder die Auswirkungen des Vorfalls rechtzeitig abschwächen.
- Identifizieren Sie die erwarteten Aktivitätsmuster für Ihre Arbeitsbelastung.Legen Sie auf der Grundlage Ihrer Kennzahlen Muster für die Workload-Aktivität fest, um unerwartetes Verhalten zu erkennen und gegebenenfalls mit geeigneten Maßnahmen zu reagieren.AWSbietetTools zur Überwachungdie statistische und maschinelle Lernalgorithmen anwenden, um Metriken zu analysieren und Anomalien zu erkennen.
- Warnung, wenn Workload-Anomalien festgestellt werden.Wenn Anomalien im Betrieb von Amazon RDS-Workloads festgestellt werden, lösen Sie eine Warnung aus, damit Sie bei Bedarf mit geeigneten Maßnahmen reagieren können.
- Überprüfen und überarbeiten Sie KPIs und Kennzahlen. Vergewissern Sie sich, dass Ihre Amazon RDS-Datenbanken Ihre definierten Anforderungen erfüllen, und identifizieren Sie Bereiche, in denen Verbesserungen möglich sind, um Ihre Geschäftsziele zu erreichen. Validieren Sie die Effektivität der gemessenen Metriken und bewerteten KPIs und überarbeiten Sie sie gegebenenfalls. Nehmen wir zum Beispiel an, Sie legen einen KPI für die optimale Anzahl gleichzeitiger Datenbankverbindungen fest und überwachen Messwerte für versuchte und fehlgeschlagene Verbindungen sowie Benutzerthreads, die erstellt wurden und ausgeführt werden. Möglicherweise haben Sie mehr Datenbankverbindungen als die, die in Ihrer KPI-Baseline definiert sind. Durch die Analyse Ihrer aktuellen Kennzahlen können Sie das Ergebnis erkennen, aber möglicherweise nicht die Ursache ermitteln. In diesem Fall sollten Sie Ihre Metriken überarbeiten und zusätzliche Überwachungsmaßnahmen einbeziehen, z. B. Zähler für Tabellensperren. Die neuen Metriken würden dabei helfen, festzustellen, ob die erhöhte Anzahl von Datenbankverbindungen auf unerwartete Tabellensperren zurückzuführen ist.

# Überwachungstools

Wir empfehlen, dass Sie Tools für Beobachtbarkeit, Überwachung und Warnung verwenden, um:

- Gewinnen Sie Einblicke in die Leistung Ihrer Amazon RDS-Umgebung
- Erkennen Sie unerwartetes und verdächtiges Verhalten
- Kapazität planen und fundierte Entscheidungen über die Zuweisung von Amazon RDS-Instances treffen
- Analysieren Sie Metriken und Protokolle, um potenzielle Probleme proaktiv vorherzusagen
- Generieren Sie Warnmeldungen, wenn Schwellenwerte überschritten werden, um Probleme zu beheben und zu lösen, bevor Ihre Benutzer davon betroffen sind

Sie haben verschiedene Optionen und Lösungen zur Auswahl, darunter von AWS bereitgestellte, Cloud-native Observability- und Monitoring-Tools und -Services, kostenlose Open-Source-Softwarelösungen und kommerzielle Drittanbieterlösungen für die Überwachung von Amazon RDS-DB-Instances. Einige dieser Tools werden in den folgenden Abschnitten behandelt.

Um herauszufinden, welches Tool Ihren Anforderungen am besten entspricht, vergleichen Sie die Funktionen und Fähigkeiten der einzelnen Tools mit den Anforderungen Ihres Unternehmens. Wir empfehlen Ihnen außerdem, die Tools im Hinblick auf einfache Bereitstellung, Konfiguration und Integration, Softwareupdates und Wartung, Bereitstellungsmethode (z. B. Hardware oder serverlos), Lizenzierung, Preis und alle anderen Faktoren, die für Ihr Unternehmen spezifisch sind, zu bewerten.

Sections

# In Amazon RDS enthaltene Tools

Amazon Relational Database Service (Amazon RDS) ist ein verwalteter Datenbankservice in der AWS-Cloud. Da es sich bei Amazon RDS um einen verwalteten Service handelt, werden Sie von den meisten Verwaltungsaufgaben wie Datenbank-Backups, Betriebssystem- (OS) und Datenbanksoftwareinstallationen, Betriebssystem- und Software-Patches, Hochverfügbarkeitseinrichtung, Hardware-Lebenszyklus und Rechenzentrumsbetrieb befreit. AWS bietet außerdem eine umfassende Reihe von Tools, mit denen Sie eine vollständige Observability-Lösung für Ihre Amazon RDS-DB-Instances erstellen können.

Einige der Überwachungstools sind im Amazon RDS-Service enthalten, vorkonfiguriert und automatisch aktiviert. Sobald Sie Ihre neue Amazon RDS-Instance starten, stehen Ihnen zwei automatisierte Tools zur Verfügung:

- Der Amazon RDS-Instance-Status bietet Details zum aktuellen Zustand Ihrer DB-Instance. Zu den Statuscodes gehören beispielsweise Verfügbar, Gestoppt, Erstellt, Sicherung und Fehlgeschlagen. Sie können die Amazon RDS-Konsole, die AWS Command Line Interface (AWS CLI) oder die Amazon RDS-API verwenden, um den Instance-Status zu sehen. Weitere Informationen finden Sie unter Amazon RDS-DB-Instance-Status anzeigen in der Amazon RDS-Dokumentation.
- Amazon RDS-Empfehlungen bieten automatisierte Empfehlungen für DB-Instances, Read Replicas und DB-Parametergruppen. Diese Empfehlungen basieren auf der Analyse der Nutzung, der Leistungsdaten und der Konfiguration von DB-Instances und dienen als Leitfaden. Die Empfehlung zur veralteten Engine-Version deutet beispielsweise darauf hin, dass auf Ihren DB-Instances nicht die neueste Version der Datenbanksoftware ausgeführt wird und dass Sie Ihre DB-Instance aktualisieren sollten, um von den neuesten Sicherheitsupdates und anderen Verbesserungen zu profitieren. Weitere Informationen finden Sie unter Amazon RDS-Empfehlungen anzeigen in der Amazon RDS-Dokumentation.

# CloudWatch Namespaces

Amazon RDS ist in Amazon integriert CloudWatch, einen Überwachungs- und Warndienst für Cloud-Ressourcen und -Anwendungen, die auf AWS ausgeführt werden. Amazon RDS sammelt automatisch Metriken, Protokolldateien, Traces und Ereignisse über den Betrieb, die Nutzung, die Leistung und den Zustand von DB-Instances und sendet sie CloudWatch zur Langzeitspeicherung, Analyse und Warnung an.

Amazon RDS for MySQL und Amazon RDS for MariaDB veröffentlichen automatisch CloudWatch in Intervallen von einer Minute ohne zusätzliche Kosten einen Standardsatz von Metriken. Diese Metriken werden in zwei Namespaces gesammelt, die Container für Metriken sind:

- Der AWS/RDS-Namespace umfasst Metriken auf DB-Instance-Ebene. Beispiele hierfür sind `BinLogDiskUsage` (die Menge an Festplattenspeicher, die von Binärprotokollen belegt wird), `CPUUtilization` (der Prozentsatz der CPU-Auslastung), `DatabaseConnections` (die Anzahl der Client-Netzwerkverbindungen zur DB-Instance) und viele mehr.
- Der AWS/Usage-Namespace enthält Nutzungsmetriken auf Kontoebene, anhand derer ermittelt wird, ob Sie innerhalb Ihrer Amazon RDS-Servicekontingente arbeiten. Beispiele hierfür sind `DBInstances` (die Anzahl der DB-Instances in Ihrem AWS-Konto oder Ihrer Region), `DBSubnetGroups` (die Anzahl der DB-Subnetzgruppen in Ihrem AWS Konto oder Ihrer Region) und `ManualSnapshots` (die Anzahl der manuell erstellten Datenbank-Snapshots in Ihrem AWS Konto oder Ihrer Region).

CloudWatch speichert Metrikdaten wie folgt:

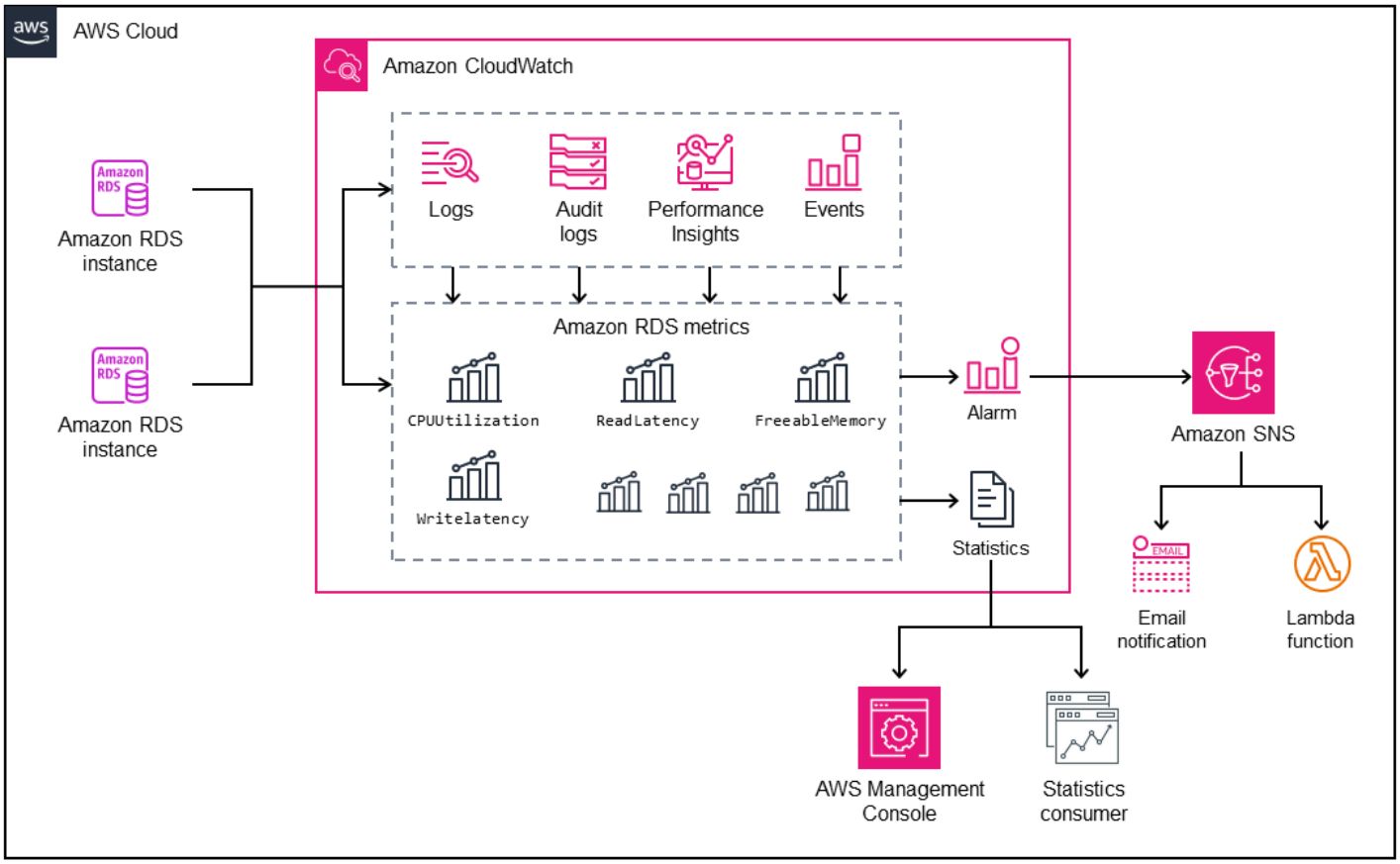
- 3 Stunden: Hochauflösende benutzerdefinierte Messwerte mit einem Zeitraum von weniger als 60 Sekunden werden 3 Stunden lang aufbewahrt. Nach 3 Stunden werden die Datenpunkte zu Kennzahlen für einen Zeitraum von 1 Minute zusammengefasst und 15 Tage lang aufbewahrt.
- 15 Tage: Datenpunkte mit einem Zeitraum von 60 Sekunden (1 Minute) werden 15 Tage lang aufbewahrt. Nach 15 Tagen werden die Datenpunkte zu Kennzahlen für einen Zeitraum von 5 Minuten zusammengefasst und 63 Tage lang aufbewahrt.
- 63 Tage: Datenpunkte mit einem Zeitraum von 300 Sekunden (5 Minuten) werden 63 Tage lang aufbewahrt. Nach 63 Tagen werden die Datenpunkte zu Kennzahlen für einen Zeitraum von einer Stunde zusammengefasst und 15 Monate lang aufbewahrt.
- 15 Monate: Datenpunkte mit einem Zeitraum von 3.600 Sekunden (1 Stunde) sind für 15 Monate (455 Tage) verfügbar.

Weitere Informationen finden Sie in der CloudWatch Dokumentation unter Metriken.

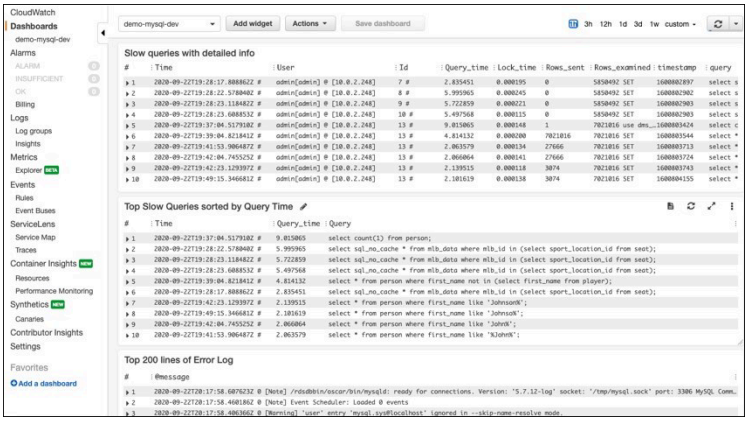
## CloudWatch Alarme und Dashboards

Sie können Amazon CloudWatch Alarms verwenden, um eine bestimmte Amazon RDS-Metrik über einen bestimmten Zeitraum zu beobachten. Sie können beispielsweise überwachen und dann eine

oder mehrere Aktionen ausführen`FreeStorageSpace`, wenn der Wert der Metrik den von Ihnen festgelegten Schwellenwert überschreitet. Wenn Sie den Schwellenwert auf 250 MB setzen und der freie Speicherplatz 200 MB beträgt (weniger als der Schwellenwert), wird der Alarm aktiviert und kann eine Aktion auslösen, um automatisch zusätzlichen Speicher für die Amazon RDS-DB-Instance bereitzustellen. Der Alarm kann mithilfe von Amazon Simple Notification Service (Amazon SNS) auch eine Benachrichtigungs-SMS an den DBA senden. Das folgende Diagramm veranschaulicht diesen Prozess.

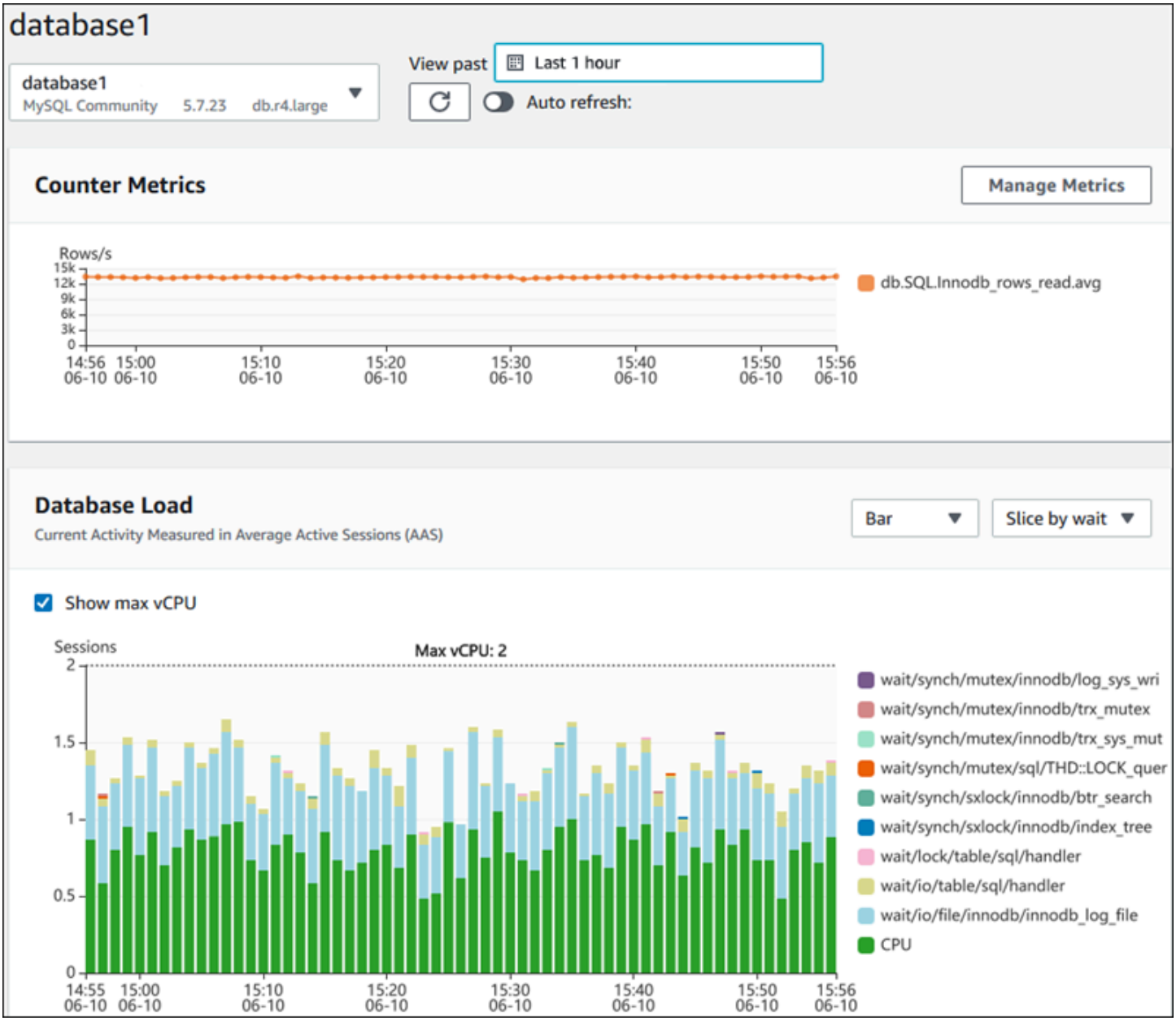



CloudWatch bietet auch Dashboards, mit denen Sie benutzerdefinierte Ansichten (Grafiken) der Metriken erstellen, anpassen, mit ihnen interagieren und sie speichern können. Sie können CloudWatch Logs Insights auch verwenden, um ein Dashboard zur Überwachung des Protokolls für langsame Abfragen und des Fehlerprotokolls zu erstellen und Benachrichtigungen zu erhalten, wenn in diesen Protokollen ein bestimmtes Muster erkannt wurde. Der folgende Bildschirm zeigt ein CloudWatch Beispiel-Dashboard.




# Amazon RDS Performance Insights

Amazon RDS Performance Insights ist ein Tool zur Optimierung und Überwachung der Datenbankleistung, das die Überwachungsfunktionen von Amazon RDS erweitert. Es hilft Ihnen bei der Analyse der Leistung Ihrer Datenbank, indem es die Auslastung der DB-Instance visualisiert und die Last nach Wartezeiten, SQL-Anweisungen, Hosts oder Benutzern filtert. Das Tool kombiniert mehrere Metriken in einem einzigen interaktiven Diagramm, das Ihnen hilft, die Art von Engpässen zu identifizieren, die Ihre DB-Instance haben könnte, wie z. B. Lock-Waits, hohe CPU-Auslastung oder I/O-Latenz, und zu ermitteln, welche SQL-Anweisungen den Engpass verursachen. Der folgende Bildschirm zeigt eine Beispielvisualisierung.




Sie müssen Performance Insights während der Erstellung der DB-Instance aktivieren, um Metriken für die Amazon RDS-DB-Instances in Ihrem Konto zu sammeln. Das kostenlose Kontingent umfasst sieben Tage Leistungsdatenverlauf und eine Million API-Anfragen pro Monat. Optional können Sie längere Aufbewahrungsfristen erwerben. Umfassende Informationen zur Preisgestaltung finden Sie unter Performance Insights – Preise.

Informationen darüber, wie Sie Performance Insights zur Überwachung Ihrer DB-Instances verwenden können, finden Sie im Abschnitt DB-Instance-Überwachung weiter unten in diesem Handbuch.

Performance Insights veröffentlicht automatisch Metriken für CloudWatch. Sie können nicht nur das Performance Insights Insights-Tool verwenden, sondern auch die zusätzlichen Funktionen nutzen, die es CloudWatch bietet. Sie können die Performance Insights Insights-Metriken mithilfe der CloudWatch Konsole AWS CLI, der oder der CloudWatch API untersuchen. Wie bei allen anderen Metriken können Sie auch CloudWatch Alarme hinzufügen. Möglicherweise möchten Sie beispielsweise eine SMS-Benachrichtigung an DBAs auslösen oder eine Abhilfemaßnahme ergreifen, wenn die `DBLoad` Metrik den von Ihnen festgelegten Schwellenwert überschreitet. Sie können die Performance Insights Insights-Metriken auch zu Ihren vorhandenen CloudWatch Dashboards hinzufügen.

## Verbesserte Überwachung

Enhanced Monitoring ist ein Tool, das Metriken für das Betriebssystem (OS), auf dem Ihre Amazon RDS-DB-Instance läuft, in Echtzeit erfasst. Diese Metriken bieten unter anderem eine Granularität von bis zu einer Sekunde für CPU-, Arbeitsspeicher-, Amazon RDS- und Betriebssystemprozesse, Dateisystem- und Festplatten-I/O-Daten. Sie können in der Amazon RDS-Konsole auf diese Metriken zugreifen und sie analysieren. Wie bei Performance Insights werden Enhanced Monitoring-Metriken von Amazon RDS an übermittelt CloudWatch, wo Sie von zusätzlichen Funktionen wie der langfristigen Aufbewahrung von Metriken für Analysen, der Erstellung von Metrikfiltern, der Anzeige von Diagrammen im CloudWatch Dashboard und der Einrichtung von Alarmen profitieren können. Standardmäßig ist Enhanced Monitoring deaktiviert, wenn Sie eine neue Amazon RDS-DB-Instance erstellen. Sie können die Funktion aktivieren, wenn Sie eine DB-Instance erstellen oder ändern. Die Preise basieren auf der Menge der Daten, die von Amazon RDS in CloudWatch Logs übertragen werden, und auf den Speichergebühren. Abhängig von der Granularität und der Anzahl der DB-Instances, für die Enhanced Monitoring aktiviert ist, kann ein Teil der Überwachungsdaten in das kostenlose Kontingent für CloudWatch Logs aufgenommen werden. Vollständige Preisinformationen finden Sie unter CloudWatch Amazon-Preise. Weitere Informationen zu dem Tool finden Sie in der Amazon RDS-Dokumentation und in den häufig gestellten Fragen zu Enhanced Monitoring.

## Zusätzliche AWS Dienste

AWS bietet mehrere unterstützende Services, die auch in Amazon RDS integriert werden können CloudWatch, um die Beobachtbarkeit Ihrer Datenbanken weiter zu verbessern. Dazu gehören Amazon EventBridge, Amazon CloudWatch Logs und AWS CloudTrail.

- Amazon EventBridge ist ein serverloser Event-Bus, der Ereignisse aus Ihren Anwendungen und AWS Ressourcen, einschließlich Ihrer Amazon RDS-DB-Instances, empfangen, filtern,

transformieren, weiterleiten und bereitstellen kann. Ein Amazon RDS-Ereignis weist auf eine Änderung in der Amazon RDS-Umgebung hin. Wenn beispielsweise eine DB-Instance ihren Status von Verfügbar auf Gestoppt ändert, generiert Amazon RDS das Ereignis`RDS-EVENT-0087 / The DB instance has been stopped`. Amazon RDS übermittelt Ereignisse an CloudWatch Events und das nahezu EventBridge in Echtzeit. Mit EventBridge und CloudWatch Events können Sie Regeln definieren, um Benachrichtigungen zu bestimmten Amazon RDS-Ereignissen von Interesse zu senden und Aktionen zu automatisieren, die ergriffen werden, wenn ein Ereignis der Regel entspricht. Als Reaktion auf ein Ereignis stehen eine Vielzahl von Zielen zur Verfügung, z. B. eine AWS Lambda Funktion, die eine Korrekturmaßnahme durchführen kann, oder ein Amazon SNS SNS-Thema, das eine E-Mail oder SMS senden kann, um DBAs oder DevOps Techniker über das Ereignis zu informieren.

- Amazon CloudWatch Logs ist ein Service, der die Speicherung von Protokolldateien aus all Ihren Anwendungen, Systemen und AWS Services zentralisiert, einschließlich Amazon RDS for MySQL- und MariaDB-DB-Instances und. AWS CloudTrail Wenn Sie die Funktion für Ihre DB-Instances aktivieren, veröffentlicht Amazon RDS automatisch die folgenden CloudWatch Protokolle in Logs:
  - Fehler-log
  - Slow-Query-Protokoll
  - Allgemeines Protokoll
  - Prüfungsprotokoll

  Sie können CloudWatch Logs Insights verwenden, um die Protokolldaten abzufragen und zu analysieren. Die Funktion umfasst eine speziell entwickelte Abfragesprache, mit der Sie nach Protokollereignissen suchen können, die den von Ihnen definierten Mustern entsprechen. Sie können beispielsweise die Beschädigung von Tabellen in Ihrer MySQL-DB-Instance verfolgen, indem Sie die Fehlerprotokolldatei auf das folgende Muster überprüfen:`"ERROR 1034 (HY000): Incorrect key file for table '*'; try to repair it OR Table * is marked as crashed"`. Gefilterte Protokolldaten können in CloudWatch Metriken umgewandelt werden. Sie können die Metriken dann verwenden, um Dashboards mit Grafiken oder Tabellendaten zu erstellen oder einen Alarm einzustellen, wenn der definierte Schwellenwert überschritten wird. Dies ist besonders nützlich, wenn Sie das Auditprotokoll verwenden, da Sie es automatisch überwachen, Warnmeldungen senden und Korrekturmaßnahmen ergreifen können, wenn ein unerwartetes oder verdächtiges Verhalten festgestellt wird. Sie können mit der AWS Management Console, der Amazon RDS-API oder dem AWS CLI AWS SDK for CloudWatch Logs auf Datenbankprotokolle zugreifen und diese verwalten.

- AWS CloudTrailprotokolliert und überwacht kontinuierlich die Benutzer- und API-Aktivitäten in Ihrem AWS-Konto. Es unterstützt Sie bei der Prüfung, Sicherheitsüberwachung und betrieblichen Fehlerbehebung Ihrer Amazon RDS for MySQL- oder MariaDB-DB-Instances. CloudTrail ist in Amazon RDS integriert. Alle Aktionen können protokolliert werden und CloudTrail bietet eine Aufzeichnung der Aktionen, die von einem Benutzer, einer Rolle oder einem AWS Service in Amazon RDS ausgeführt wurden. Wenn ein Benutzer beispielsweise eine neue Amazon RDS-DB-Instance erstellt, wird ein Ereignis erkannt, und das Protokoll enthält Informationen über die angeforderte Aktion (`"eventName": "CreateDBInstance"`), Datum und Uhrzeit der Aktion (`"eventTime": "2022-07-30T22:14:06Z"`), Anforderungsparameter (`"requestParameters": {"dBInstanceIdentifier": "test-instance", "engine": "mysql", "dBInstanceClass": "db.m6g.large"}`) usw. Zu den Ereignissen, die von protokolliert werden, CloudTrail gehören sowohl Aufrufe von der Amazon RDS-Konsole als auch Aufrufe von Code, der die Amazon RDS-API verwendet.

## Überwachungstools von Drittanbietern

In einigen Szenarien möchten Sie möglicherweise zusätzlich zu der vollständigen Suite von Cloud-nativen Observabilitäts- und Überwachungstools, die Amazon RDS AWS bietet, Überwachungstools von anderen Softwareanbietern verwenden. Zu diesen Szenarien gehören Hybridbereitstellungen, bei denen möglicherweise eine Reihe von Datenbanken in Ihrem lokalen Rechenzentrum und eine weitere Gruppe von Datenbanken in dem ausgeführt werden. AWS Cloud Wenn Sie Ihre Observability-Lösung für Ihr Unternehmen bereits eingerichtet haben, möchten Sie möglicherweise weiterhin Ihre vorhandenen Tools verwenden und sie auf Ihre AWS-Cloud-Bereitstellungen ausweiten. Die Herausforderung bei der Einrichtung einer Überwachungslösung eines Drittanbieters liegt häufig in den Sicherheitsvorkehrungen, die Amazon RDS als Cloud-verwalteter Service auferlegt. Sie können beispielsweise keine Agentsoftware auf dem Host-Betriebssystem installieren, auf dem die DB-Instance ausgeführt wird, da der Zugriff auf den Datenbank-Host-Computer verweigert wird. Sie können jedoch viele Überwachungslösungen von Drittanbietern in Amazon RDS integrieren, indem Sie auf anderen AWS Cloud Diensten aufbauen. CloudWatch Beispielsweise können Amazon RDS-Metriken, Protokolle, Ereignisse und Traces exportiert und dann zur weiteren Analyse, Visualisierung und Alarmierung in das Überwachungstool eines Drittanbieters importiert werden. Einige dieser Drittanbieterlösungen umfassen Prometheus, Grafana und Percona.

## Prometheus und Grafana

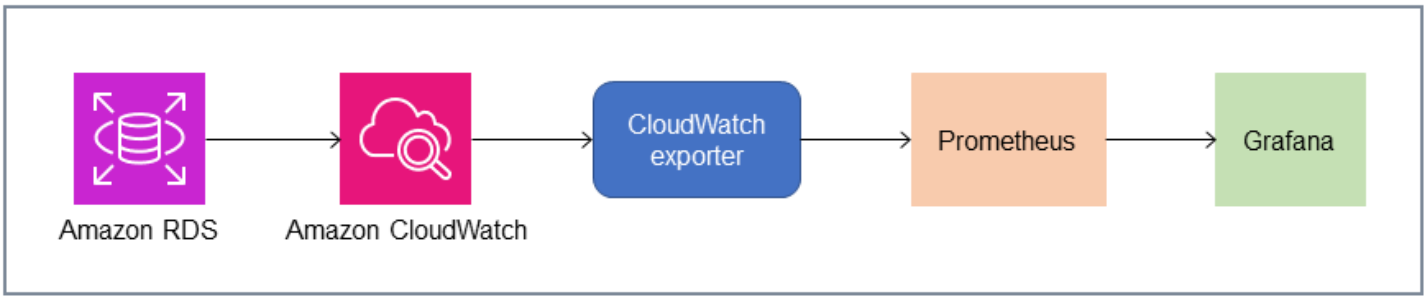
Prometheus ist eine Open-Source-Monitoring-Lösung, die in bestimmten Intervallen Metriken von konfigurierten Zielen sammelt. Es handelt sich um eine Allzweck-Überwachungslösung, mit der jede Anwendung oder jeder Dienst überwacht werden kann. Wenn Sie Amazon RDS-DB-Instances überwachen, CloudWatch sammelt die Metriken von Amazon RDS. Die Metriken werden dann mithilfe eines Open-Source-Exporters wie YACE Exporter oder Exporter auf den Prometheus-Server exportiert. CloudWatch

- Der YACE Exporter optimiert Datenexportaufgaben, indem er mehrere Metriken in einer einzigen Anfrage an die API abruft. CloudWatch Nachdem die Messwerte auf dem Prometheus-Server gespeichert wurden, wertet der Server Regelausdrücke aus und kann Warnmeldungen generieren, wenn bestimmte Bedingungen eingehalten werden.
- CloudWatch Exporter wird offiziell von Prometheus betrieben. Es ruft CloudWatch Metriken über die CloudWatch API ab und speichert sie auf dem Prometheus-Server in einem Format, das mit Prometheus kompatibel ist, indem es REST-API-Anfragen an den HTTP-Endpunkt verwendet.

Wenn Sie einen Exporter auswählen, Ihr Bereitstellungsmodell entwerfen und Exporter-Instanzen konfigurieren, sollten Sie Service CloudWatch- und API-Kontingente berücksichtigen und CloudWatch protokollieren, da der Export von CloudWatch Metriken auf einen Prometheus-Server zusätzlich zur API implementiert wird. CloudWatch Beispielsweise könnte die Bereitstellung mehrerer CloudWatch Exporter-Instances in einer einzigen AWS-Konto Region zur Überwachung von Hunderten von Amazon RDS-DB-Instances zu einem Drosselungsfehler (ThrottlingException) und zu Code-400-Fehlern führen. Um solche Einschränkungen zu überwinden, sollten Sie den YACE Exporter in Betracht ziehen, der für die Erfassung von bis zu 500 verschiedenen Metriken in einer einzigen Anfrage optimiert ist. Um eine große Anzahl von Amazon RDS-DB-Instances bereitzustellen, sollten Sie außerdem erwägen, mehrere zu verwenden AWS-Konten, anstatt die Arbeitslast in einer einzigen AWS-Konto zu zentralisieren und die Anzahl der Exporter-Instances in jeder zu begrenzen. AWS-Konto

Alerts werden vom Prometheus-Server generiert und vom Alertmanager bearbeitet. Dieses Tool kümmert sich um die Deduplizierung, Gruppierung und Weiterleitung von Warnmeldungen an den richtigen Empfänger wie E-Mail, SMS oder Slack oder leitet eine automatische Antwortaktion ein. Ein anderes Open-Source-Tool namens Grafana zeigt Visualisierungen für diese Metriken an. Grafana bietet umfangreiche Visualisierungs-Widgets wie erweiterte Grafiken, dynamische Dashboards und Analysefunktionen wie Ad-hoc-Abfragen und dynamischen Drilldown. Es kann auch

Protokolle durchsuchen und analysieren und enthält Warnfunktionen zur kontinuierlichen Auswertung von Metriken und Protokollen sowie zum Senden von Benachrichtigungen, wenn die Daten den Warnungsregeln entsprechen.




## Percona

Percona Monitoring and Management (PMM) ist eine kostenlose Open-Source-Lösung zur Datenbanküberwachung, -verwaltung und -beobachtbarkeit für MySQL und MariaDB. PMM sammelt Tausende von Leistungsmetriken von DB-Instances und ihren Hosts. Es bietet eine Weboberfläche zur Visualisierung von Daten in Dashboards und zusätzliche Funktionen wie automatische Berater für die Bewertung des Datenbankzustands. Sie können PMM verwenden, um Amazon RDS zu überwachen. Der PMM-Client (Agent) ist jedoch nicht auf den zugrunde liegenden Hosts der Amazon RDS-DB-Instances installiert, da er keinen Zugriff auf die Hosts hat. Stattdessen stellt das Tool eine Verbindung zu den Amazon RDS-DB-Instances her, fragt Serverstatistiken`INFORMATION_SCHEMA`, das Systemschema und das Leistungsschema ab und verwendet die CloudWatch API, um Metriken, Protokolle, Ereignisse und Traces zu erfassen. PMM benötigt einen AWS Identity and Access Management (IAM-) Benutzerzugriffsschlüssel (IAM-Rolle) und erkennt automatisch die Amazon RDS-DB-Instances, die für die Überwachung verfügbar sind. Das PMM-Tool ist für die Datenbanküberwachung konzipiert und sammelt mehr datenbankspezifische Metriken als Prometheus. Um das PMM Query Analytics-Dashboard zu verwenden, müssen Sie das Performance-Schema als Abfragequelle konfigurieren, da der Query Analytics-Agent nicht für Amazon RDS installiert ist und das langsame Abfrageprotokoll nicht lesen kann. Stattdessen fragt es direkt die `performance_schema` von den MySQL- und MariaDB-DB-Instances ab, um Metriken zu erhalten. Eines der herausragenden Merkmale von PMM ist die Fähigkeit, DBAs bei Problemen zu warnen und zu beraten, die das Tool in ihren Datenbanken identifiziert. PMM bietet eine Reihe von Prüfungen, mit denen allgemeine Sicherheitsbedrohungen, Leistungseinbußen, Datenverlust und Datenbeschädigung erkannt werden können.

Zusätzlich zu diesen Tools sind auf dem Markt mehrere kommerzielle Beobachtungs- und Überwachungslösungen erhältlich, die in Amazon RDS integriert werden können. Beispiele hierfür

sind Datadog Database Monitoring, Dynatrace Amazon RDS Monitoring und Database Monitoring. AppDynamics

# Überwachung von DB-Instances

EINDB-Instanceist der grundlegende Baustein von Amazon RDS. Es ist eine isolierte Datenbankumgebung, die in der Cloud läuft. Für MySQL- und MariaDB-Datenbanken ist die DB-InstancemysqldProgramm, auch bekannt als MySQL-Server, das mehrere Threads und Komponenten wie den SQL-Parser, den Abfrageoptimierer, den Thread-/Verbindungs-Handler, System- und Statusvariablen sowie eine oder mehrere steckbare Speicher-Engines umfasst. Jede Speicher-Engine ist so konzipiert, dass sie einen speziellen Anwendungsfall unterstützt. Die standardmäßige und empfohlene Speicher-Engine istInnoDB, eine transaktionale, universelle, relationale Datenbank-Engine, die dem ACID-Modell (Atomizity, Consistency, Isolation, Duristability) entspricht. InnoDB-FunktionenIn-Memory-Strukturen(Pufferpool, Change-Puffer, adaptiver Hash-Index, Log-Puffer) sowieStrukturen auf der Festplatte(Tablespaces, Tabellen, Indizes, Undo-Log, Redo-Log, Doublewrite-Pufferdateien). Um sicherzustellen, dass Ihre Datenbank genau dem ACID-Modell entspricht,Die InnoDB-Speicher-Engine implementiert zahlreiche Funktionenum Ihre Daten zu schützen, einschließlich Transaktionen, Commit, Rollback, Crash-Recovery, Sperren auf Zeilenebene und Multiversion Concurrency Control (MVCC).

All diese internen Komponenten einer DB-Instance arbeiten zusammen, um die Verfügbarkeit, Integrität und Sicherheit Ihrer Daten auf dem erwarteten und zufriedenstellenden Leistungsniveau aufrechtzuerhalten. Abhängig von Ihrer Arbeitslast kann jede Komponente und Funktion Ressourcenanforderungen an CPU-, Arbeitsspeicher-, Netzwerk- und Speichersubsysteme stellen. Wenn ein Anstieg der Nachfrage nach einer bestimmten Ressource die bereitgestellte Kapazität oder die Softwarelizenzen für diese Ressource übersteigt (entweder aufgrund von Konfigurationsparametern oder durch das Softwaredesign), kann es bei der DB-Instance zu Leistungseinbußen oder zu vollständiger Nichtverfügbarkeit und Beschädigung kommen. Daher ist es wichtig, diese internen Komponenten zu messen und zu überwachen, sie mit definierten Basiswerten zu vergleichen und Warnmeldungen zu generieren, wenn die überwachten Werte von den erwarteten Werten abweichen.

Wie zuvor beschrieben, können Sie verschiedene verwendenWerkzeugeum Ihre MySQL- und MariaDB-Instanzen zu überwachen. Wir empfehlen Ihnen, Amazon RDS Performance Insights zu verwenden undCloudWatchTools für Überwachung und Warnmeldungen, da diese Tools in Amazon RDS integriert sind, hochauflösende Metriken erfassen, die neuesten Leistungsinformationen nahezu in Echtzeit präsentieren und Alarme generieren.

Unabhängig von Ihrem bevorzugten Überwachungstool empfehlen wir Ihnen,schalten Sie das Leistungsschema einin Ihren MySQL- und MariaDB-DB-Instances. DerLeistungsschemaist

eine optionale Funktion zur Überwachung des Betriebs des MySQL-Servers (der DB-Instance) auf niedriger Ebene. Sie ist so konzipiert, dass sie nur minimale Auswirkungen auf die Gesamtleistung der Datenbank hat. Sie können diese Funktion verwalten, indem Sie den`performance_schema`Parameter. Dieser Parameter ist zwar optional, Sie müssen ihn jedoch verwenden, um hochauflösende (eine Sekunde) pro SQL-Metriken, aktive Sitzungsmetriken, Warteereignisse und andere detaillierte Überwachungsinformationen auf niedriger Ebene zu erfassen, die von Amazon RDS Performance Insights erfasst werden.

Sektionen



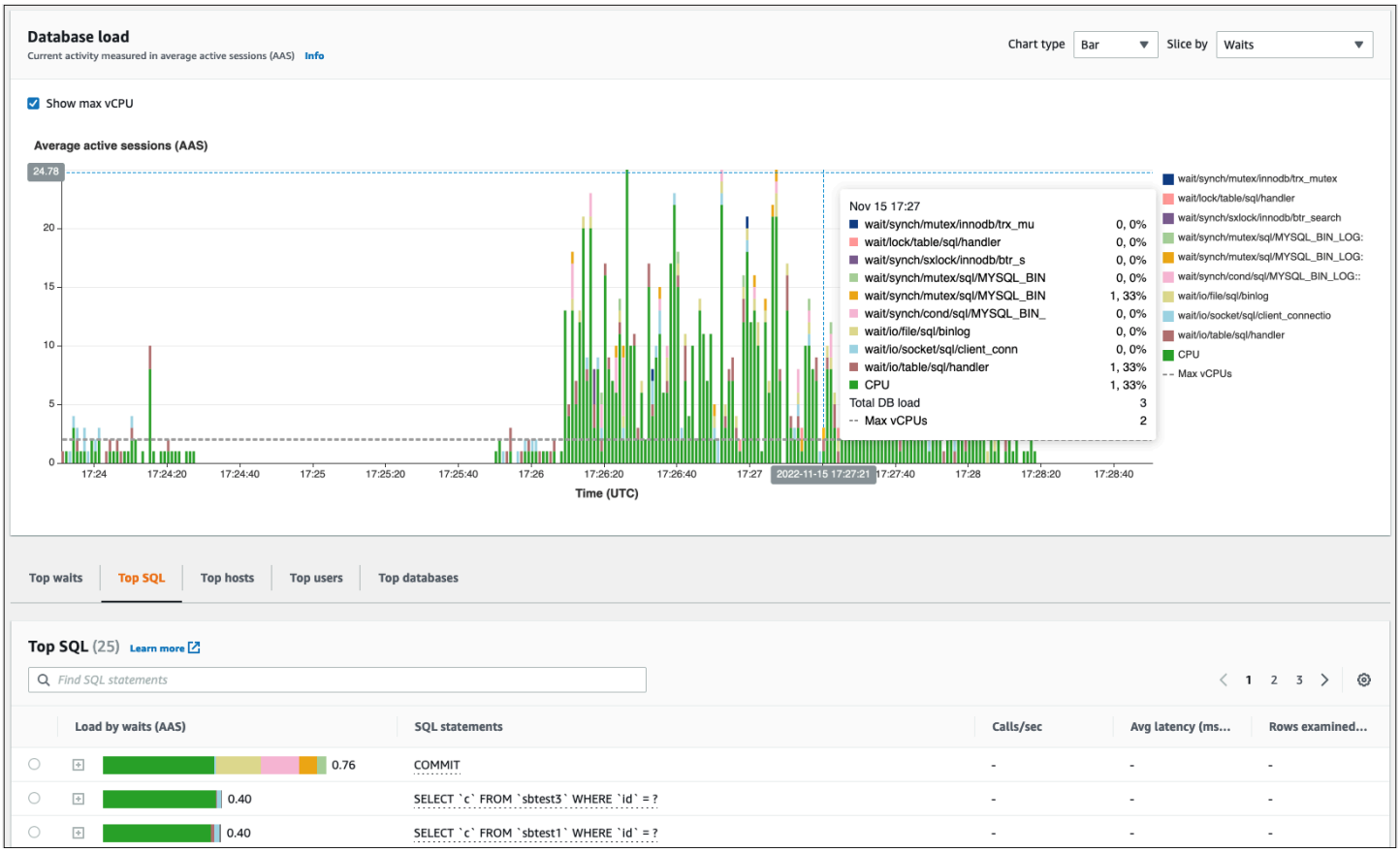
# Performance Insights-Metriken für DB-Instances

Performance Insights überwacht verschiedene Arten von Metriken, wie in den folgenden Abschnitten beschrieben.

## Datenbanklast

Datenbanklast (`DBLoad`) ist eine wichtige Metrik in Performance Insights, mit der das Aktivitätsniveau in Ihrer Datenbank gemessen wird. Es wird jede Sekunde gesammelt und automatisch auf Amazon veröffentlicht.CloudWatch. Es stellt die Aktivität der DB-Instance in durchschnittlichen aktiven Sessions (AAS) dar. Dies ist die Anzahl der Sitzungen, in denen gleichzeitig SQL-Abfragen ausgeführt werden. Der`DBLoad`Die Metrik unterscheidet sich von anderen Zeitreihenmetriken, da sie mithilfe einer dieser fünf Dimensionen interpretiert werden kann: Waits, SQL, Hosts, Benutzer und Datenbanken. Diese Dimensionen sind Unterkategorien der`DBLoad`metrisch. Sie können sie verwenden alsschneiden nachKategorien, um verschiedene Merkmale der Datenbanklast darzustellen. Eine ausführliche Beschreibung, wie wir die Datenbanklast berechnen, finden Sie unterDatenbanklastin der Amazon RDS-Dokumentation.

Die folgende Bildschirmabbildung zeigt das Performance Insights-Tool.




## Dimensionen

- Ereignisse abwartensind Bedingungen, unter denen eine Datenbanksitzung auf den Abschluss einer Ressource oder eines anderen Vorgangs wartet, um die Verarbeitung fortzusetzen. Wenn Sie eine SQL-Anweisung ausführen wie`SELECT * FROM big_table`und wenn diese Tabelle viel größer ist als der zugewiesene InnoDB-Pufferpool, wird Ihre Sitzung höchstwahrscheinlich warten`wait/io/file/innodb/innodb_data_file`Warteereignisse, die durch physische I/O-Operationen in der Datendatei verursacht werden. Warteereignisse sind eine wichtige Dimension für die Datenbanküberwachung, da sie auf mögliche Leistungsengpässe hinweisen. Wait-Ereignisse geben die Ressourcen und Operationen an, auf die die SQL-Anweisungen, die Sie in Sitzungen ausführen, die meiste Zeit warten. Zum Beispiel die`wait/synch/mutex/innodb/trx_sys_mutex`Ereignis tritt ein, wenn eine hohe Datenbankaktivität mit einer großen Anzahl von Transaktionen vorliegt und die`wait/synch/mutex/innodb/buf_pool_mutex`Ereignis tritt ein, wenn ein Thread eine Sperre für den InnoDB-Pufferpool erlangt hat, um auf eine Seite im Speicher zuzugreifen. Hinweise zu allen MySQL- und MariaDB-Warteereignissen finden Sie unterÜbersichtstabellen für Warteereignissein der MySQL-Dokumentation. Informationen zur

Interpretation von Instrumentennamen finden Sie unterNamenskonventionen für Leistungsschema-Instrumentein der MySQL-Dokumentation.

- SQLzeigt, welche SQL-Anweisungen am meisten zur gesamten Datenbanklast beitragen. DerTop-AbmessungenTabelle, die sich unter demDatenbanklastDas Diagramm in Amazon RDS Performance Insights ist interaktiv. Eine detaillierte Liste der Warteereignisse im Zusammenhang mit der SQL-Anweisung erhalten Sie, indem Sie auf die Leiste in derNach Wartezeiten laden (AAS)Spalte. Wenn Sie eine SQL-Anweisung in der Liste auswählen, zeigt Performance Insights die zugehörigen Warteereignisse in derDatenbanklastDiagramm und der Text der SQL-Anweisung in derSQL-TextAbschnitt. SQL-Statistiken werden auf der rechten Seite des angezeigtTop-AbmessungenTabelle.
- Gastgeberzeigt die Hostnamen der verbundenen Clients an. Diese Dimension hilft Ihnen zu erkennen, welche Client-Hosts die meiste Last an die Datenbank senden.
- Nutzergruppiert die DB-Last nach Benutzern, die in der Datenbank angemeldet sind.
- Datenbankengruppiert die DB-Last nach dem Namen der Datenbank, mit der der Client verbunden ist.

## Zähler-Metriken

Zählerkennzahlen sind kumulative Metriken, deren Werte nur erhöht oder auf Null zurückgesetzt werden können, wenn die DB-Instance neu gestartet wird. Der Wert einer Zählermetrik kann nicht auf ihren vorherigen Wert reduziert werden. Diese Kennzahlen stellen einen einzigen, monoton ansteigenden Zähler dar.

- Systemeigene Zählersind Metriken, die von der Datenbank-Engine und nicht von Amazon RDS definiert werden. Beispiele:
  - `SQL.Innodb_rows_inserted`stellt die Anzahl der Zeilen dar, die in InnoDB-Tabellen eingefügt wurden.
  - `SQL.Select_scan`steht für die Anzahl der Joins, die einen vollständigen Scan der ersten Tabelle abgeschlossen haben.
  - `Cache.Innodb_buffer_pool_reads`steht für die Anzahl der logischen Lesevorgänge, die die InnoDB-Engine nicht aus dem Pufferpool abrufen konnte und direkt von der Festplatte lesen musste.
  - `Cache.Innodb_buffer_pool_read_requests`steht für die Anzahl der logischen Leseanforderungen.

Definitionen aller systemeigenen Metriken finden Sie unterServerstatusvariablenin der MySQL-Dokumentation.

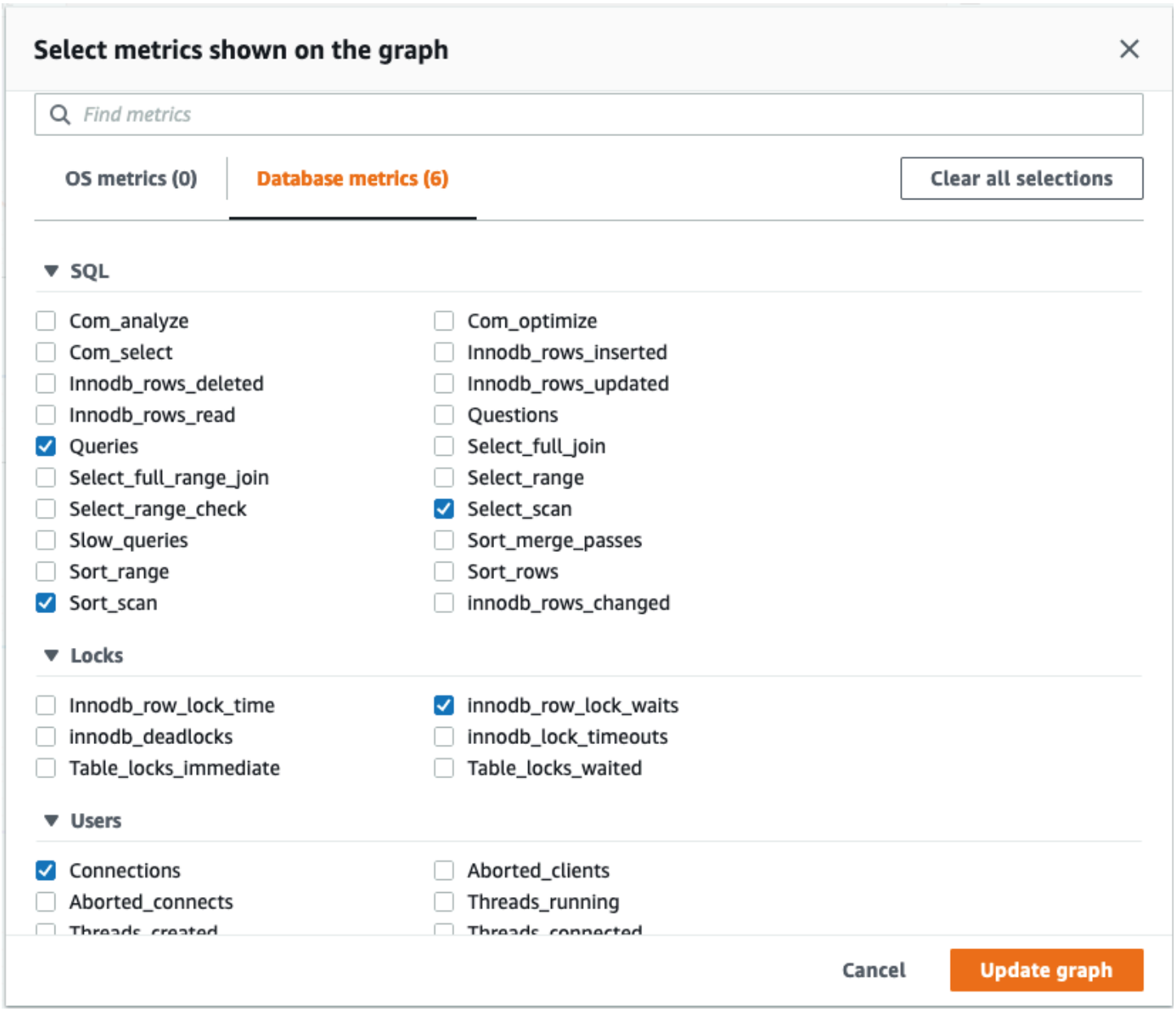
- Leistungsindikatoren, die nicht systemintern sindwerden von Amazon RDS definiert. Sie können diese Metriken entweder mithilfe einer bestimmten Abfrage abrufen oder sie ableiten, indem Sie zwei oder mehr systemeigene Metriken in Berechnungen verwenden. Nicht systemeigene Zählerkennzahlen können Latenzen, Kennzahlen oder Trefferquoten darstellen. Beispiele:
  - `Cache.innoDB_buffer_pool_hits`stellt die Anzahl der Leseoperationen dar, die InnoDB aus dem Pufferpool abrufen könnte, ohne die Festplatte zu verwenden. Er wird anhand der systemeigenen Zählerkennzahlen wie folgt berechnet:

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

  - `IO.innoDB_datafile_writes_to_disk`stellt die Anzahl der Schreibvorgänge von InnoDB-Datendateien auf die Festplatte dar. Es erfasst nur Operationen auf Datendateien — keine Schreibvorgänge mit Doublewrite oder Redo-Logging. Sie wird wie folgt berechnet:

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

Sie können DB-Instance-Metriken direkt im Performance Insights-Dashboard visualisieren. Wählen SieKennzahlen verwalten, wähle denDatenbank-Metrikenklicken Sie auf die Tabulatortaste und wählen Sie dann die gewünschten Kennzahlen aus, wie in der folgenden Abbildung dargestellt.




Wählen Sie dieGrafik aktualisierenSchaltfläche, um die ausgewählten Metriken anzuzeigen, wie in der folgenden Abbildung dargestellt.


## SQL-Statistiken

Performance Insights sammelt leistungsbezogene Metriken zu SQL-Abfragen für jede Sekunde, in der eine Abfrage ausgeführt wird, und für jeden SQL-Aufruf. Im Allgemeinen sammelt Performance InsightsSQL-Statistikauf der Ebene der Aussage und der Zusammenfassung. Für MariaDB- und MySQL-DB-Instances werden Statistiken jedoch nur auf der Digest-Ebene erfasst.

- Die Digest-Statistik ist eine zusammengesetzte Metrik aller Abfragen, die dasselbe Muster haben, aber letztendlich unterschiedliche Literalwerte haben. Der Digest ersetzt bestimmte Literalwerte durch eine Variable, zum Beispiel:

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

- Es gibt Kennzahlen, die Statistiken darstellenpro Sekundefür jede verdaute SQL-Anweisung. Zum Beispiel`sql_tokenized.stats.count_star_per_sec`steht für Aufrufe pro Sekunde (das heißt, wie oft pro Sekunde die SQL-Anweisung ausgeführt wurde).

- Performance Insights umfasst auch Kennzahlen, die Folgendes bieten:pro AnrufStatistiken für eine SQL-Anweisung. Zum Beispiel`sql_tokenized.stats.sum_timer_wait_per_call`zeigt die durchschnittliche Latenz der SQL-Anweisung pro Aufruf in Millisekunden.

SQL-Statistiken sind im Performance Insights-Dashboard verfügbar, in derTop-SQLReiter desTop-AbmessungenTabelle.


## CloudWatchMetriken für DB-Instances

AmazonasCloudWatchenthält auch Metriken, die Amazon RDS automatisch veröffentlicht. Die Metriken, die sich in der`AWS/RDS`Namespace sindMetriken auf Instanzebene, was sich auf die Amazon RDS (Service) -Instance (d. h. die isolierte Datenbankumgebung, die in der Cloud ausgeführt wird) und nicht auf die DB-Instance im engeren Sinne desmysqldverarbeiten. Daher die meisten von denenStandardmetrikenfallen in der strengen Definition des Begriffs unter die Kategorie der Betriebssystemmetriken. Zu den Beispielen gehören:`CPUUtilization`,`WriteIOPS`,`SwapUsage`und andere. Dennoch gibt es einige DB-Instance-Metriken, die auf MariaDB und MySQL anwendbar sind:

- `BinLogDiskUsage`— Die Menge an Festplattenspeicher, die von Binärprotokollen belegt wird.
- `DatabaseConnections`— Die Anzahl der Client-Netzwerkverbindungen zur DB-Instance.
- `ReplicaLag`— Die Zeit, in der eine Read Replica-DB-Instance hinter der Quell-DB-Instance zurückbleibt.

## Veröffentlichung von Performance Insights-Metriken fürCloudWatch

Amazon RDS Performance Insights überwacht die meisten Metriken und Dimensionen der DB-Instance und stellt sie über das Performance Insights-Dashboard imAWSManagement-Konsole. Dieses Dashboard eignet sich gut für die Fehlerbehebung in Datenbanken und die Ursachenanalyse.

Es ist jedoch nicht möglich, in Performance Insights Alarme für leistungsbezogene Kennzahlen zu erstellen. Um Alarme auf der Grundlage von Performance Insights-Metriken zu erstellen, müssen Sie diese Metriken verschieben inCloudWatch. Die Metriken habenCloudWatchbietet Ihnen auch Zugriff auf erweiterte Überwachungsfunktionen wieCloudWatchErkennung von Anomalien,metrische Mathematik, undStatistiken, und Sie können die Metriken in externe Überwachungstools wie Prometheus und Grafana exportieren.

Performance Insights-Metriken werden nicht automatisch unter veröffentlichtCloudWatch(mit Ausnahme derdbLoad-Metrik). Um die DB-Instance-Metriken von Performance Insights zu veröffentlichenCloudWatch, du kannst das benutzenAPI für Leistungseinblickeum Metriken abzurufen, undCloudWatchAPIum Metriken zu veröffentlichen fürCloudWatch. Um den Prozess zu automatisieren, können Sie eine Lambda-Funktion erstellen und sie in Amazon planen.EventBridgeum zu bestimmten Zeiträumen zu laufen, z. B. alle zwei Minuten. Sie können angeben, für welche Performance Insights-Metriken Sie veröffentlichen möchten.CloudWatch. Die Lambda-Funktion ruft diese Metriken von allen Amazon RDS-Instances ab, für die Performance Insights aktiviert ist, und speichert die Metriken inCloudWatch. Weitere Informationen zu diesem Prozess finden Sie im Blogbeitrag überBereitstellung von Performance Insights Leistungskennzahlen fürCloudWatch.

# Betriebssystemüberwachung

Eine DB-Instance in Amazon RDS für MySQL oder MariaDB läuft auf dem Linux-Betriebssystem, das die zugrunde liegenden Systemressourcen nutzt: CPU, Arbeitsspeicher, Netzwerk und Speicher.

```
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)
```

Die Gesamtleistung Ihrer Datenbank und des zugrunde liegenden Betriebssystems hängen stark von der Auslastung der Systemressourcen ab. Beispielsweise ist die CPU die Schlüsselkomponente für die Leistung Ihres Systems, da sie die Anweisungen der Datenbanksoftware ausführt und andere Systemressourcen verwaltet. Wenn die CPU überbeansprucht wird (das heißt, wenn die Last mehr CPU-Leistung erfordert, als für Ihre DB-Instance bereitgestellt wurde), würde sich dieses Problem auf die Leistung und Stabilität Ihrer Datenbank und damit auf Ihre Anwendung auswirken.

Die Datenbank-Engine weist dynamisch Speicher zu und gibt ihn frei. Wenn im RAM nicht genügend Speicher vorhanden ist, um die aktuelle Arbeit zu erledigen, schreibt das System Speicherseiten in den Swap-Speicher, der sich auf der Festplatte befindet. Da die Festplatte viel langsamer ist als der Arbeitsspeicher, selbst wenn die Festplatte auf der SSD-NVMe-Technologie basiert, führt eine übermäßige Speicherzuweisung zu Leistungseinbußen. Eine hohe Speicherauslastung führt zu einer erhöhten Latenz der Datenbankantworten, da die Größe einer Seitendatei wächst, um zusätzlichen Speicher zu unterstützen. Wenn die Speicherzuweisung so hoch ist, dass sowohl der RAM als auch der Swap-Speicherplatz erschöpft sind, ist der Datenbankdienst möglicherweise nicht mehr verfügbar, und Benutzer könnten Fehler beobachten, wie`[ERROR] mysqld: Out of memory (Needed xyz bytes)`.

MySQL- und MariaDB-Datenbankverwaltungssysteme verwenden das Speichersubsystem, das aus Festplatten besteht, die speichernStrukturen auf der Festplattewie Tabellen, Indizes, Binärprotokolle, Redo-Logs, Undo-Logs und Doublewrite-Pufferdateien. Daher muss die Datenbank im Gegensatz zu

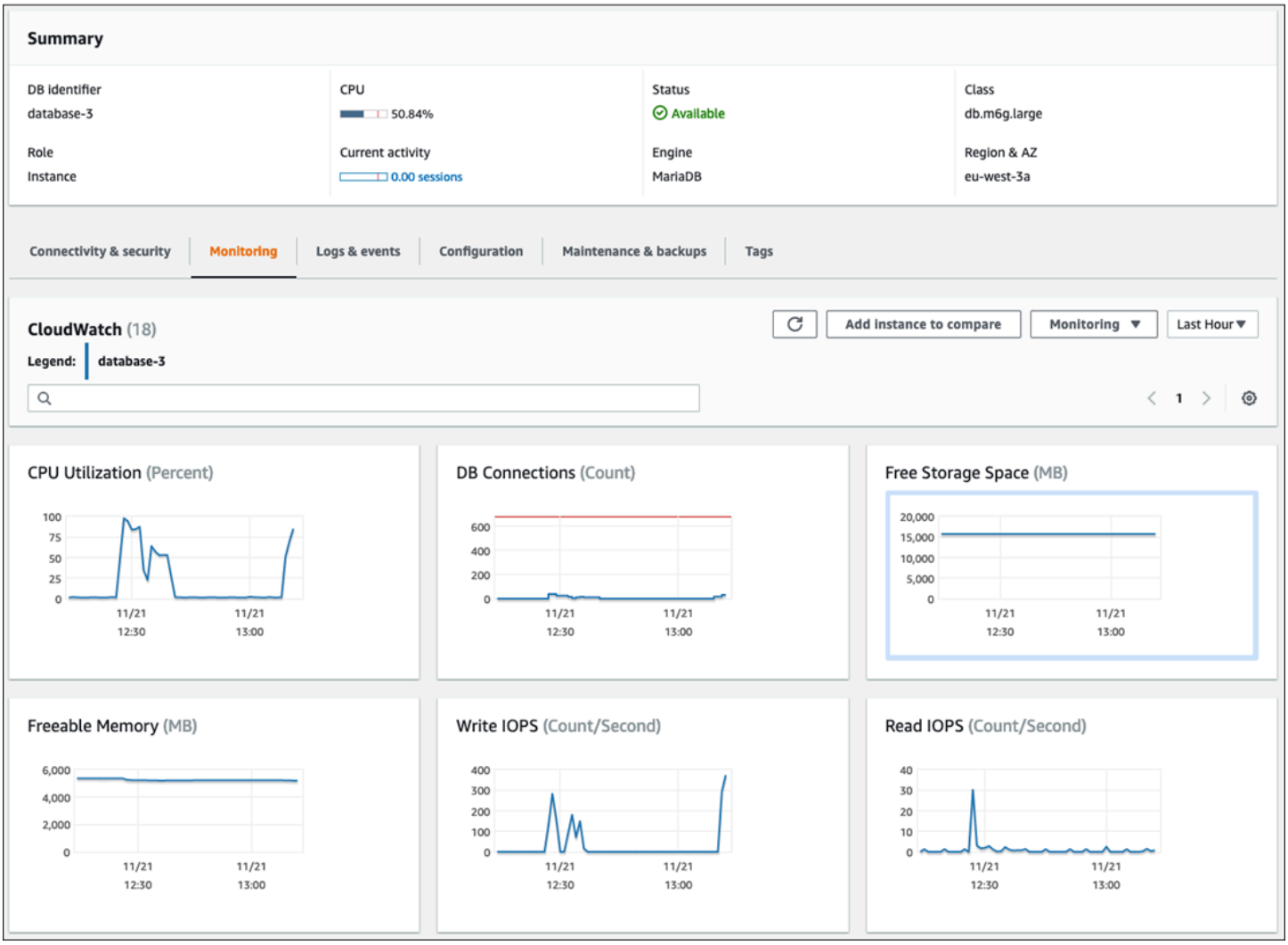
anderen Softwaretypen viel Festplattenaktivität ausführen. Für den optimalen Betrieb Ihrer Datenbank ist es wichtig, dass Sie die Festplatten-I/O-Auslastung und die Festplattenspeicherzuweisung überwachen und optimieren. Die Datenbankleistung kann beeinträchtigt werden, wenn die Datenbank die von der Festplatte unterstützten maximalen IOPS oder des maximalen Durchsatzes erreicht. Beispielsweise können durch einen Indexscan verursachte Bursts von zufälligen Zugriffen zu einer großen Anzahl von I/O-Vorgängen pro Sekunde führen, was letztendlich an die Grenzen des zugrunde liegenden Speichers stoßen könnte. Bei vollständigen Tabellenscans wird das IOPS-Limit möglicherweise nicht erreicht, aber sie können zu einem hohen Durchsatz führen, der in Megabyte pro Sekunde gemessen wird. Es ist wichtig, die Speicherplatzzuweisung zu überwachen und Warnmeldungen zu generieren, da Fehler wie`OS error code 28: No space left on device`kann zur Nichtverfügbarkeit und Beschädigung der Datenbank führen.

Amazon RDS stellt in Echtzeit Metriken für das Betriebssystem bereit, auf dem Ihre DB-Instance ausgeführt wird. Amazon RDS veröffentlicht automatisch einen Satz von Betriebssystemmetriken fürCloudWatch. Diese Metriken stehen Ihnen zur Anzeige und Analyse in der Amazon RDS-Konsole und imCloudWatchDashboards, und Sie können Alarme für die ausgewählten Metriken einrichten inCloudWatch. Beispiele sind unter anderem:

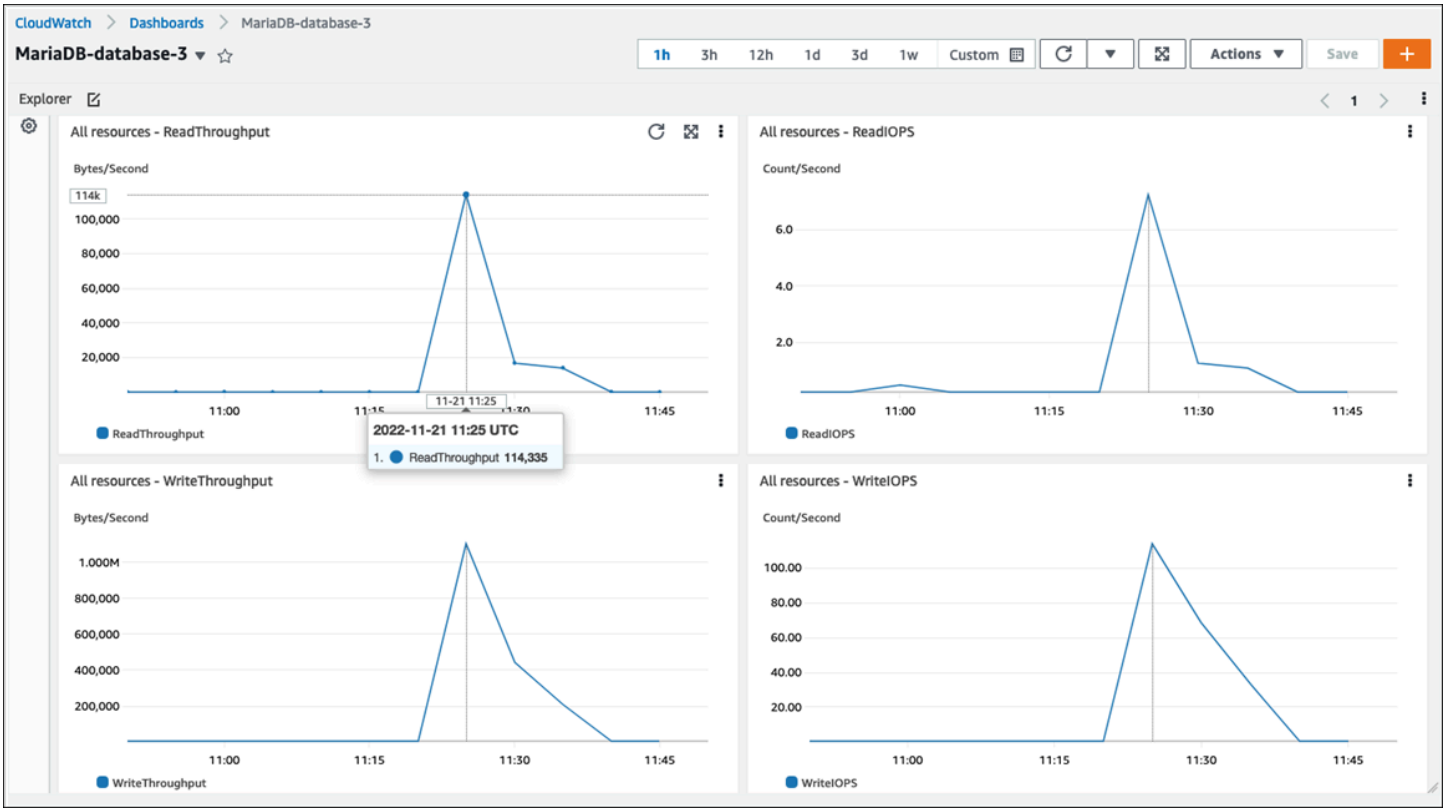
- `CPUUtilization`— Der Prozentsatz der CPU-Auslastung.
- `BinLogDiskUsage`— Die Menge an Festplattenspeicher, die von Binärprotokollen belegt wird.
- `FreeableMemory`— Die Menge des verfügbaren Direktzugriffsspeichers. Dies entspricht dem Wert des`MemAvailable`Feld von`/proc/meminfo`.
- `ReadIOPS`— Die durchschnittliche Anzahl von Festplatten-E/A-Lesevorgängen pro Sekunde.
- `WriteThroughput`— Die durchschnittliche Anzahl von Byte, die pro Sekunde für den lokalen Speicher auf die Festplatte geschrieben werden.
- `NetworkTransmitThroughput`— Der ausgehende Netzwerkverkehr auf dem DB-Knoten, der sowohl den Datenbankverkehr als auch den Amazon RDS-Verkehr kombiniert, der für die Überwachung und Replikation verwendet wird.

Eine vollständige Referenz aller von Amazon RDS veröffentlichten Metriken finden Sie unterCloudWatch, siehe[AmazonasCloudWatchMetriken für Amazon RDS]in der Amazon RDS-Dokumentation.

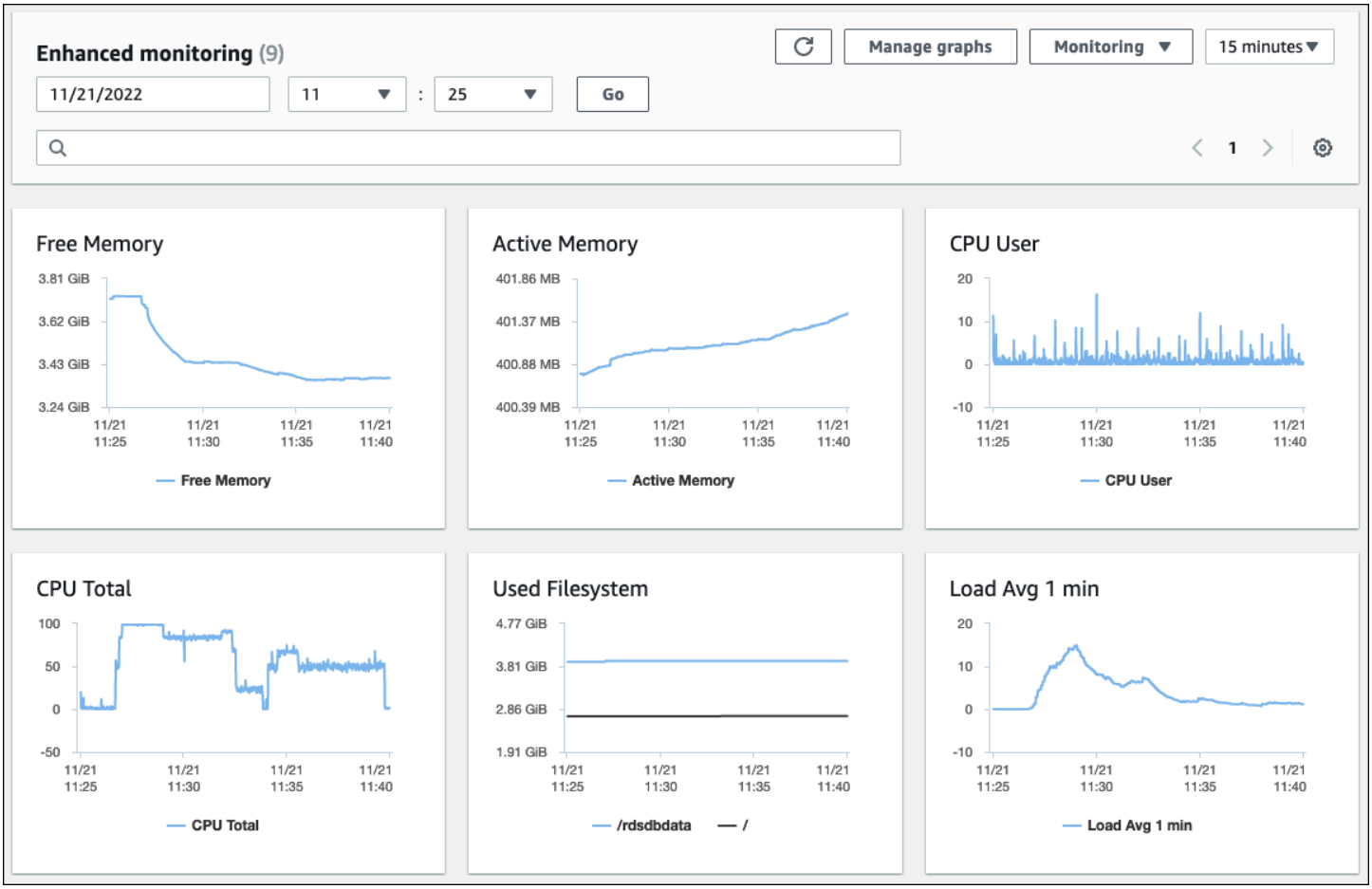
Die folgende Tabelle zeigt Beispiele fürCloudWatchMetriken für Amazon RDS, die auf der Amazon RDS-Konsole angezeigt werden.




Das folgende Diagramm zeigt ähnliche Metriken, die in derCloudWatchArmaturenbrett.




Der andere Satz von Betriebssystemmetriken wird gesammelt vonVerbesserte Überwachungfür Amazon RDS. Dieses Tool bietet Ihnen einen besseren Einblick in den Zustand Ihrer Amazon RDS for MariaDB- und Amazon RDS for MySQL-DB-Instances, indem es Systemmetriken und Betriebssystemprozessinformationen in Echtzeit bereitstellt. Wenn duEnhanced Monitoring aktivierenauf Ihrer DB-Instance und stellen Sie die gewünschte Granularität ein. Das Tool sammelt die Betriebssystemmetriken und Prozessinformationen, die Sie auf derAmazon RDS-Konsole, wie auf dem folgenden Bildschirm gezeigt.




Einige der wichtigsten Kennzahlen, die von Enhanced Monitoring bereitgestellt werden, sind:

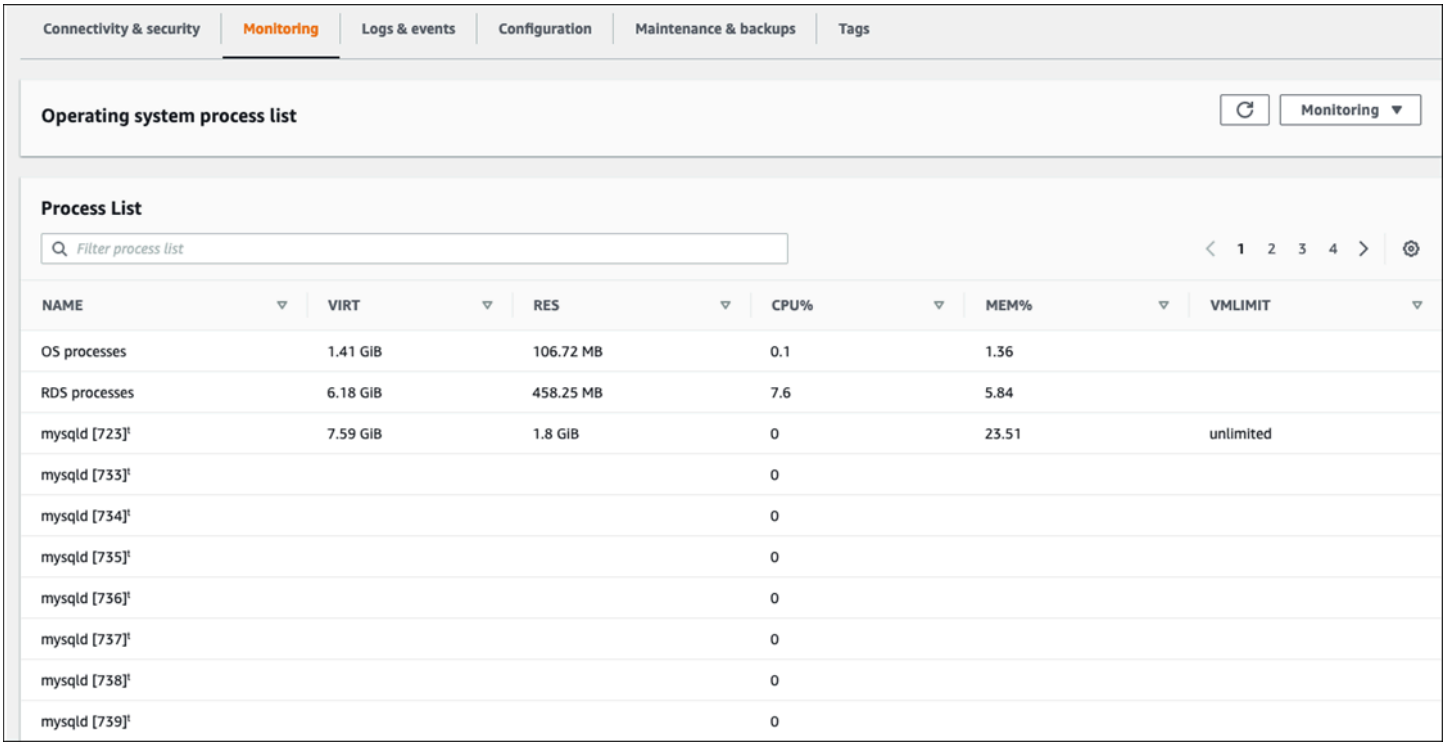
- `cpuUtilization.total`— Der Gesamtprozentsatz der verwendeten CPU.
- `cpuUtilization.user`— Der Prozentsatz der CPU, die von Benutzerprogrammen verwendet wird.
- `memory.active`— Die Menge des zugewiesenen Speichers in Kilobyte.
- `memory.cached`— Die Speichermenge, die für das Zwischenspeichern von dateisystembasierten I/O verwendet wird.
- `loadAverageMinute.one`— Die Anzahl der Prozesse, die in der letzten Minute CPU-Zeit angefordert haben.

Eine vollständige Liste der Metriken finden Sie unterBetriebssystemmetriken in Enhanced Monitoringin der Amazon RDS-Dokumentation.

In der Amazon RDS-Konsole enthält die Betriebssystemprozessliste Details zu jedem Prozess, der in Ihrer DB-Instance ausgeführt wird. Die Liste ist in drei Abschnitte unterteilt:

- Betriebssystemprozesse– Dieser Abschnitt stellt eine aggregierte Zusammenfassung aller Kernel- und Systemprozesse dar. Diese Prozesse haben im Allgemeinen nur minimale Auswirkungen auf die Datenbankleistung.
- RDS-Prozesse— Dieser Abschnitt enthält eine Zusammenfassung derAWSProzesse, die zur Unterstützung einer Amazon RDS-DB-Instance erforderlich sind. Es umfasst beispielsweise den Amazon RDS-Management-Agenten, Überwachungs- und Diagnoseprozesse und ähnliche Prozesse.
- Untergeordnete RDS-Prozesse— Dieser Abschnitt enthält eine Zusammenfassung der Amazon RDS-Prozesse, die die DB-Instance unterstützen — in diesem Fall die`mysqld`Prozess und seine Threads. Der`mysqld`Threads erscheinen verschachtelt unter dem übergeordneten`mysqld`verarbeiten.

Die folgende Bildschirmdarstellung zeigt die Liste der Betriebssystemprozesse in der Amazon RDS-Konsole.

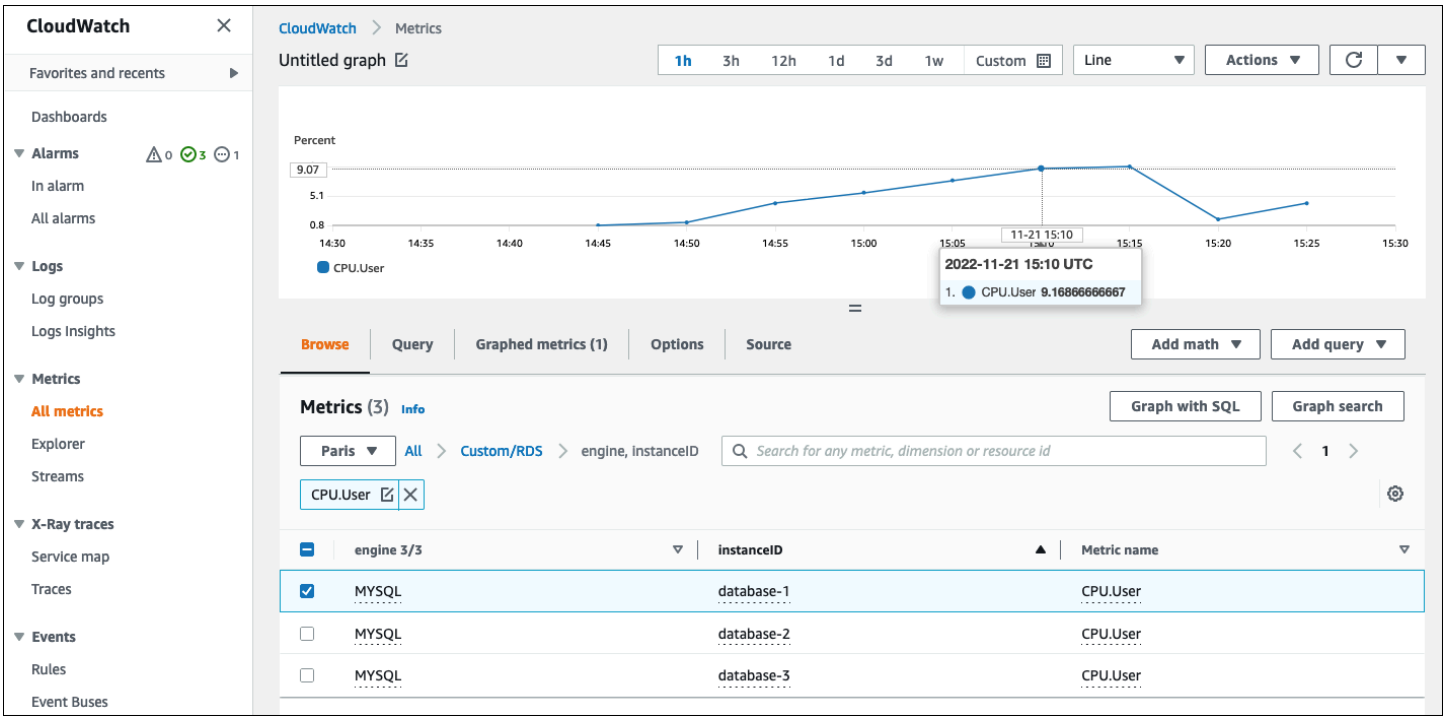



Amazon RDS liefert die Metriken von Enhanced Monitoring in IhreCloudWatchLoggt das Konto. Die Überwachungsdaten, die auf der Amazon RDS-Konsole angezeigt werden, werden abgerufen

vonCloudWatchLogs. Du kannst auchrufen Sie die Metriken für eine DB-Instance als Log-Stream abvonCloudWatchLogs. Diese Metriken werden im JSON-Format gespeichert. Sie können die JSON-Ausgabe von Enhanced Monitoring verwenden vonCloudWatchLoggt sich in ein Überwachungssystem Ihrer Wahl ein.

Um Grafiken auf dem anzuzeigenCloudWatchDashboard und Alarme erstellen, die eine Aktion auslösen würden, wenn eine Metrik den definierten Schwellenwert überschreitet, müssen Sie Metrikfilter in erstellenCloudWatchvonCloudWatchLogs. Eine ausführliche Anleitung finden Sie in derAWS re:Artikel postenzum Filtern von Enhanced MonitoringCloudWatchProtokolle zur Generierung automatisierter benutzerdefinierter Metriken für Amazon RDS.

Das folgende Beispiel veranschaulicht die benutzerdefinierte Metrik.`CPU.User`in der`Custom/RDS`Namespace. Diese benutzerdefinierte Metrik wird durch Filtern von erstellt`tcpUtilization.user`Verbesserte Überwachungsmetrik vonCloudWatchLogs.




Wenn die Metrik in der verfügbar istCloudWatchRepository, in dem Sie es anzeigen und analysieren könnenCloudWatchDashboards, wenden Sie weitere Mathematik- und Abfrageoperationen an und richten Sie einen Alarm ein, um diese spezifische Metrik zu überwachen und Warnungen zu generieren, falls die beobachteten Werte nicht den definierten Alarmbedingungen entsprechen.

# Ereignisse, Protokolle und Prüfprotokolle

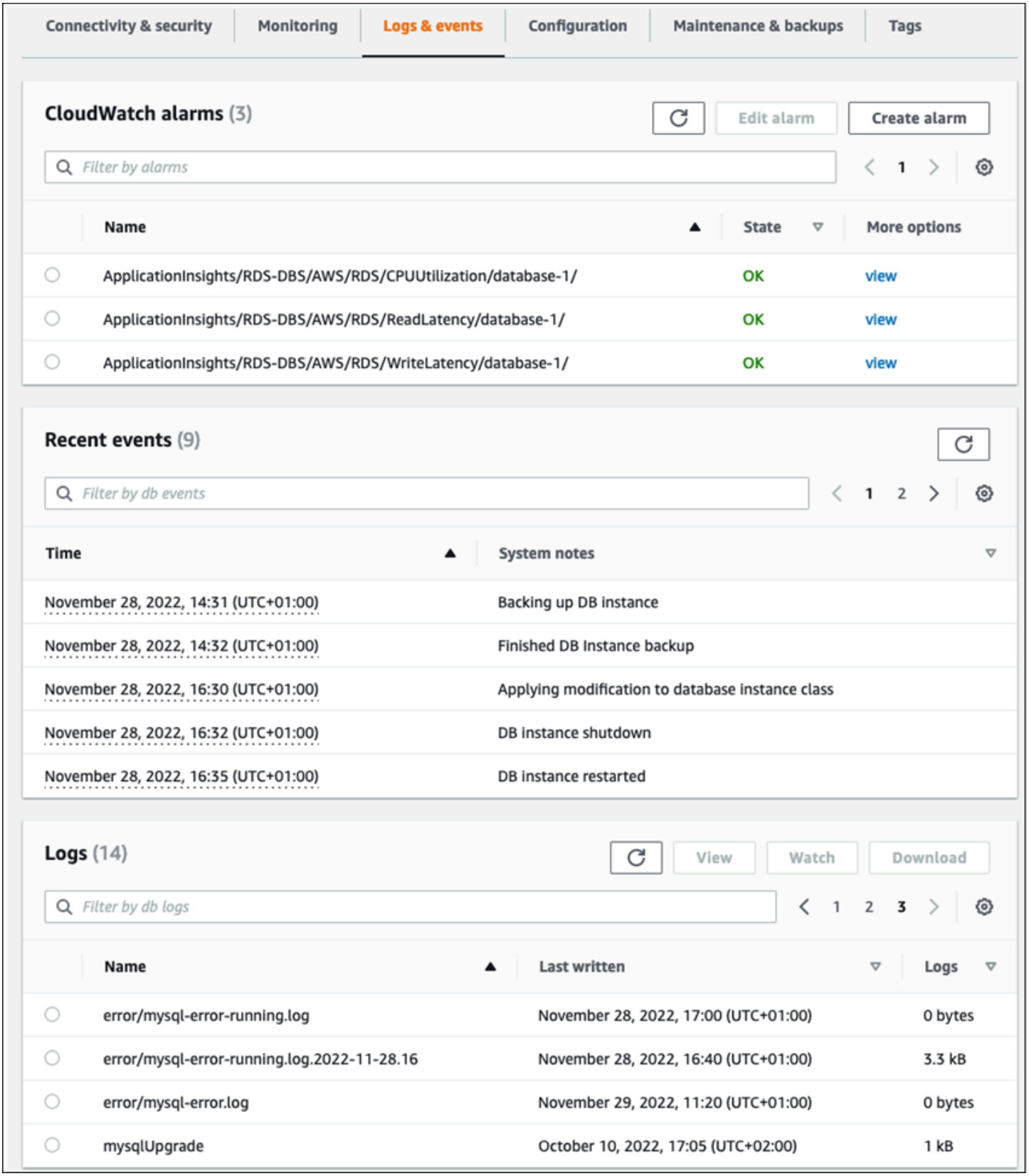
ÜberwachungDB-Instance-MetrikenundBetriebssystemmetriken, die Analyse der Trends und der Vergleich von Metriken mit Basiswerten sowie die Generierung von Warnmeldungen, wenn Werte definierte Schwellenwerte überschreiten, sind alles notwendige und bewährte Verfahren, mit denen Sie die Zuverlässigkeit, Verfügbarkeit, Leistung und Sicherheit Ihrer Amazon RDS-DB-Instances erreichen und aufrechterhalten können. Eine Komplettlösung muss jedoch auch Datenbankereignisse, Protokolldateien und Prüfprotokolle von MySQL- und MariaDB-Datenbanken überwachen.

Sektionen

- Amazon RDS-Ereignisse
- Datenbankprotokolle
- Prüfprotokolle

## Amazon RDS-Ereignisse

EinAmazonas RDS-Ereignisweist auf eine Änderung in der Amazon RDS-Umgebung hin. Zum Beispiel, wenn sich der Status der DB-Instance ändert vonBeginnendzuVerfügbar, Amazon RDS generiert das Ereignis`RDS-EVENT-0088 The DB instance has been started`. Amazon RDS übermittelt Ereignisse an AmazonEventBridgenahezu in Echtzeit. Sie können über die Amazon RDS-Konsole auf Ereignisse zugreifen, dieAWS CLIbeherrschenEreignisse beschreibenoder die Amazon RDS-API-OperationDescribeEvents. Die folgende Bildschirmdarstellung zeigt Ereignisse und Protokolle, die auf der Amazon RDS-Konsole angezeigt werden.


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

Amazon RDS sendet verschiedene Arten von Ereignissen aus, darunter DB-Instance-Ereignisse, DB-Parametergruppenereignisse, DB-Sicherheitsgruppenereignisse, DB-Snapshot-Ereignisse, RDS-Proxy-Ereignisse und blaue/grüne Bereitstellungsereignisse. Die Informationen beinhalten:

- Quellname und Quelltyp; zum Beispiel:`"SourceIdentifier": "database-1", "SourceType": "db-instance"`
- Datum und Uhrzeit des Ereignisses; zum Beispiel:`"Date": "2022-12-01T09:20:28.595000+00:00"`
- Nachricht, die mit dem Ereignis verknüpft ist, zum Beispiel:`"Message": "Finished updating DB parameter group"`
- Event-Kategorie; zum Beispiel:`"EventCategories": ["configuration change"]`

Eine vollständige Referenz finden Sie unterAmazon RDS-Ereigniskategorien und -meldungenin der Amazon RDS-Dokumentation.

Wir empfehlen, dass Sie Amazon RDS-Ereignisse überwachen, da diese Ereignisse auf Statusänderungen bei der Verfügbarkeit von DB-Instances, Konfigurationsänderungen, Read Replica-Statusänderungen, Backup- und Wiederherstellungsereignisse, Failover-Aktionen, Fehlerereignisse, Änderungen an Sicherheitsgruppen und viele andere Benachrichtigungen hinweisen. Wenn Sie beispielsweise eine Read Replica-DB-Instance eingerichtet haben, um die Leistung und Beständigkeit Ihrer Datenbank zu verbessern, empfehlen wir Ihnen, Amazon RDS-Ereignisse auf dieReplikat lesenEreigniskategorie, die DB-Instances zugeordnet ist. Das liegt daran, dass Ereignisse wie`RDS-EVENT-0057 Replication on the read replica was terminated`geben Sie an, dass Ihre Read Replica nicht mehr mit der primären DB-Instance synchronisiert wird. Eine Benachrichtigung des zuständigen Teams, dass ein solches Ereignis eingetreten ist, könnte dazu beitragen, das Problem rechtzeitig zu beheben. AmazonasEventBridgeund zusätzliche AWS-Services wieAWS Lambda, Amazon Simple Queue Service (Amazon SQS) und Amazon Simple Notification Service (Amazon SNS), können Ihnen helfen, Reaktionen auf Systemereignisse wie Probleme mit der Datenbankverfügbarkeit oder Ressourcenänderungen zu automatisieren.

Auf der Amazon RDS-Konsole können Sie Ereignisse der letzten 24 Stunden abrufen. Wenn Sie das verwendenAWS CLIoder die Amazon RDS-API zum Anzeigen von Ereignissen. Sie können Ereignisse der letzten 14 Tage abrufen, indem Sie denEreignisse beschreibenBefehl wie folgt.

```
$ 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"
        }
    ]
}
```

Wenn Sie Ereignisse langfristig speichern möchten, entweder bis zum angegebenen Ablaufzeitraum oder dauerhaft, können SieCloudWatchLogsum die Informationen über die Ereignisse zu protokollieren, die von Amazon RDS generiert wurden. Um diese Lösung zu implementieren, können Sie ein Amazon SNS-Thema verwenden, um Amazon RDS-Ereignisbenachrichtigungen zu erhalten, und dann eine Lambda-Funktion aufrufen, um das Ereignis zu protokollieren.CloudWatchProtokolle.

1. Erstellen Sie eine Lambda-Funktion, die bei dem Ereignis aufgerufen wird, und protokollieren Sie die Informationen des Ereignisses inCloudWatchProtokolle. CloudWatchLogs ist in Lambda integriert und bietet eine bequeme Möglichkeit, Ereignisinformationen zu protokollieren, indem Sie dendruckenFunktion zu`stdout`.
2. Erstellen Sie ein SNS-Thema mit einem Abonnement für eine Lambda-Funktion (Set)Protokollzu Lambda), und stellen Sie dieEndpunktzum Amazon-Ressourcennamen (ARN) der Lambda-Funktion, die Sie im vorherigen Schritt erstellt haben.
3. Konfigurieren Sie Ihr SNS-Thema, um Amazon RDS-Ereignisbenachrichtigungen zu erhalten. Eine ausführliche Anleitung finden Sie in derAWSRe: Artikel postenerfahren Sie, wie Sie Ihr Amazon SNS-Thema dazu bringen können, Amazon RDS-Benachrichtigungen zu erhalten.

4. Erstellen Sie auf der Amazon RDS-Konsole ein neues Event-Abonnement. SetZielzum ARN und wählen Sie dann das zuvor erstellte SNS-Thema aus. SetArt der QuelleundEinzufügende Veranstaltungskategoriennach Ihren Anforderungen. Weitere Informationen finden Sie unterAmazon RDS-Eventbenachrichtigung abonnierenin der Amazon RDS-Dokumentation.

## Datenbankprotokolle

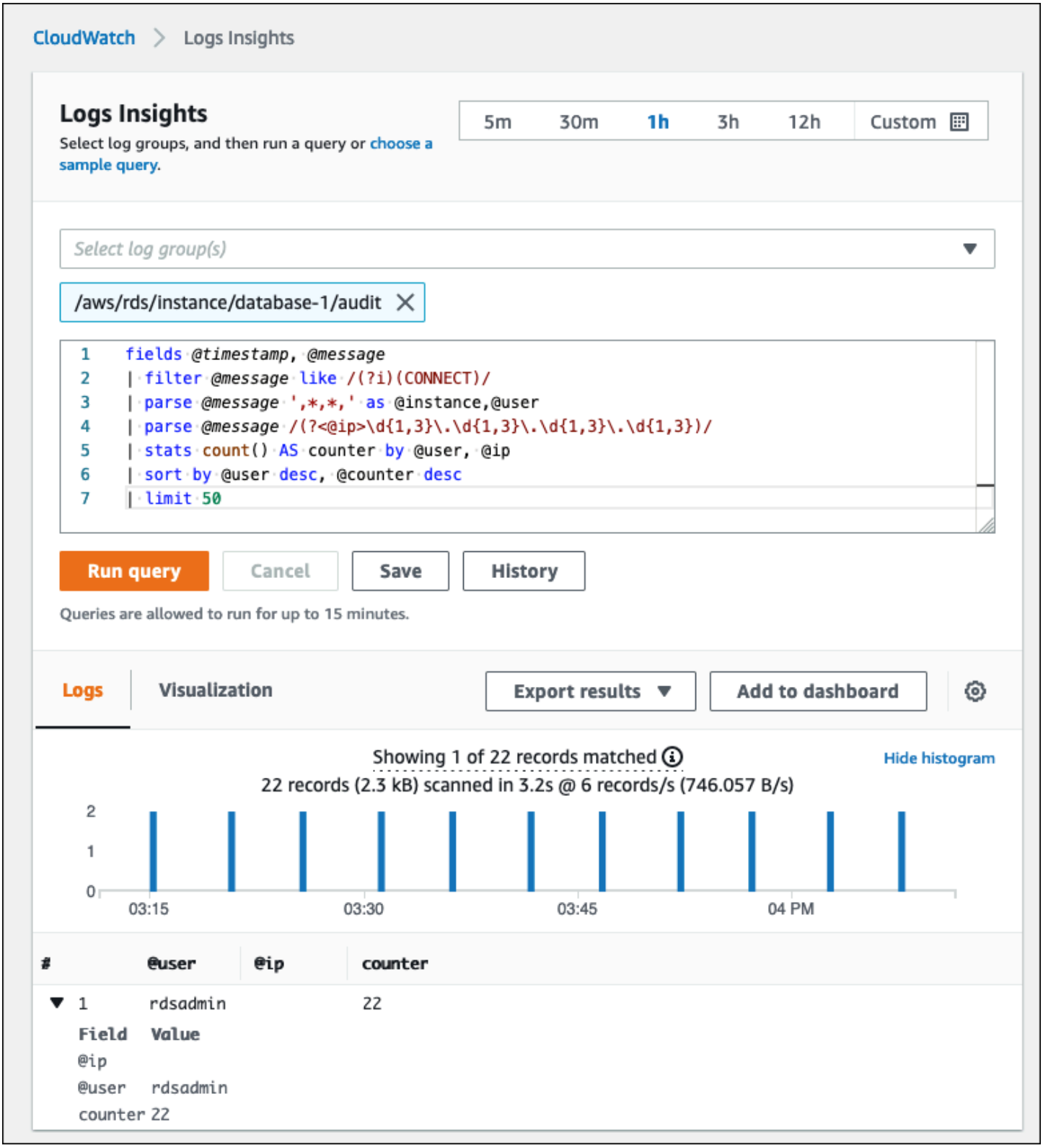
MySQL- und MariaDB-Datenbanken generieren Protokolle, auf die Sie zur Prüfung und Fehlerbehebung zugreifen können. Diese Protokolle sind:

- Prüfung— Der Audit-Trail besteht aus einer Reihe von Datensätzen, die die Aktivität des Servers protokollieren. Für jede Client-Sitzung wird aufgezeichnet, wer eine Verbindung zum Server hergestellt hat (Benutzername und Host), welche Abfragen ausgeführt wurden, auf welche Tabellen zugegriffen wurde und welche Servervariablen geändert wurden.
- Fehler— Dieses Protokoll enthält die (`mysqld`) Start- und Abschaltzeiten sowie Diagnosemeldungen wie Fehler, Warnungen und Hinweise, die beim Starten und Herunterfahren des Servers und bei laufendem Server auftreten.
- Allgemeines— Dieses Protokoll zeichnet die Aktivität von`mysqld`, einschließlich der Verbindungs- und Trennungsaktivitäten für jeden Client sowie der von Clients empfangenen SQL-Abfragen. Das allgemeine Abfrageprotokoll kann sehr nützlich sein, wenn Sie einen Fehler vermuten und genau wissen möchten, an was der Client gesendet hat`mysqld`.
- Langsame Abfrage— Dieses Protokoll enthält eine Aufzeichnung von SQL-Abfragen, deren Ausführung lange gedauert hat.

Als bewährte Methode sollten SieDatenbankprotokolle von Amazon RDS auf Amazon veröffentlichenCloudWatchLogs. MitCloudWatchProtokolle, Sie können die Protokolldaten in Echtzeit analysieren, die Daten in einem äußerst robusten Speicher speichern und die Daten verwalten mit demCloudWatchProtokolliert den Agenten. Du kannstGreifen Sie auf Ihre Datenbankprotokolle zu und beobachten Sie sievon der Amazon RDS-Konsole aus. Sie können auch verwendenCloudWatchLogs Insights zur interaktiven Suche und Analyse Ihrer Log-Daten inCloudWatchProtokolle. Das folgende Beispiel zeigt eine Abfrage im Audit-Log, die überprüft, wie oft`CONNECT`Ereignisse werden im Protokoll angezeigt, wer eine Verbindung hergestellt hat und von welchem Client (IP-Adresse) aus sie eine Verbindung hergestellt haben. Der Auszug aus dem Audit-Log könnte so aussehen:

```
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
```

Das Beispiel einer Log Insights-Abfrage zeigt das`rdsadmin`verbunden mit der Datenbank von`localhost`alle 5 Minuten, also insgesamt 22 Mal, wie in der folgenden Abbildung dargestellt. Diese Ergebnisse deuten darauf hin, dass die Aktivität von internen Amazon RDS-Prozessen wie dem Überwachungssystem selbst herrührte.




Protokollereignisse enthalten häufig wichtige Meldungen, die Sie zählen möchten, wie Warnungen oder Fehler zu Vorgängen im Zusammenhang mit MySQL- und MariaDB-DB-Instances. Schlägt

beispielsweise ein Vorgang fehl, kann ein Fehler auftreten, der wie folgt in der Fehlerprotokolldatei aufgezeichnet wird:`ERROR 1114 (HY000): The table zip_codes is full`. Möglicherweise möchten Sie diese Einträge überwachen, um den Trend Ihrer Fehler zu verstehen. Du kannstbenutzerdefiniert erstellenCloudWatchMetriken aus Amazon RDS-Protokollen mithilfe von Filternum die automatische Überwachung von Amazon RDS-Datenbankprotokollen zu ermöglichen, um ein bestimmtes Protokoll auf bestimmte Muster hin zu überwachen und bei Verstößen gegen das erwartete Verhalten einen Alarm auszulösen. Zum Beispiel, erstellen Sie einen Metrikfilter für die Protokollgruppe`/aws/rds/instance/database-1/error`das würde das Fehlerprotokoll überwachen und nach dem suchenspezifisches Muster, wie`ERROR`. Stellen Sie dieFilter-Musterzu`ERROR`undMetrischer Wertzu`1`. Der Filter erkennt jeden Protokolldatensatz, der das Schlüsselwort enthält`ERROR`, und die Anzahl wird für jedes Log-Ereignis, das „ERROR“ enthält, um 1 erhöht. Nachdem Sie den Filter erstellt haben, können Sie einen Alarm einrichten, der Sie benachrichtigt, falls Fehler im MySQL- oder MariaDB-Fehlerprotokoll erkannt werden.

Um mehr über die Überwachung des langsamen Abfrageprotokolls und des Fehlerprotokolls zu erfahren, erstellen Sie eineCloudWatchDashboard und VerwendungCloudWatchLogs Insights, siehe BlogbeitragEin Amazon erstellenCloudWatchDashboard zur Überwachung von Amazon RDS und Amazon Aurora MySQL.

## Audit-Trails

Der Audit-Trail (oder Audit-Log) bietet eine sicherheitsrelevante, chronologische Aufzeichnung der Ereignisse in Ihrem AWS-Konto. Dazu gehören Ereignisse für Amazon RDS, die dokumentarische Nachweise über die Abfolge der Aktivitäten liefern, die sich auf Ihre Datenbank oder Ihre Cloud-Umgebung ausgewirkt haben. In Amazon RDS für MySQL oder MariaDB beinhaltet die Verwendung des Audit Trails:

- Überwachung des DB-Instance-Audit-Logs
- Überwachen von Amazon RDS-API-Aufrufen inAWS CloudTrail

Für eine Amazon RDS-DB-Instance umfassen die Auditing-Ziele in der Regel:

- Aktivierung der Rechenschaftspflicht für Folgendes:
  - Änderungen, die an dem Parameter oder der Sicherheitskonfiguration vorgenommen wurden
  - Aktionen, die in einem Datenbankschema, einer Tabelle oder Zeile ausgeführt werden, oder Aktionen, die sich auf bestimmte Inhalte auswirken

- Erkennung und Untersuchung von Eindringlingen
- Erkennung und Untersuchung verdächtiger Aktivitäten
- Erkennung von Autorisierungsproblemen, z. B. um den Missbrauch von Zugriffsrechten durch reguläre oder privilegierte Benutzer zu identifizieren

Der Datenbank-Audit Trail versucht, die folgenden typischen Fragen zu beantworten:Wer hat sensible Daten in Ihrer Datenbank angesehen oder geändert? Wann ist das passiert? Von wo aus hat ein bestimmter Benutzer auf die Daten zugegriffen? Haben privilegierte Benutzer ihre uneingeschränkten Zugriffsrechte missbraucht?

Sowohl MySQL als auch MariaDB implementieren die DB-Instance Audit Trail-Funktion mithilfe des MariaDB-Audit-Plug-ins. Dieses Plugin zeichnet Datenbankaktivitäten auf, z. B. Benutzer, die sich an der Datenbank anmelden, und Abfragen, die in der Datenbank ausgeführt werden. Der Datensatz der Datenbankaktivität wird in einer Protokolldatei gespeichert. Für den Zugriff auf das Audit-Protokoll muss die DB-Instance eine benutzerdefinierte Optionsgruppe mit der Option `MARIADB_AUDIT_PLUGIN` verwenden. Weitere Informationen finden Sie unterMariaDB Audit Plugin-Unterstützung für MySQLin der Amazon RDS-Dokumentation. Die Aufzeichnungen im Audit-Log werden in einem bestimmten Format gespeichert, das vom Plugin definiert wird. Weitere Informationen zum Audit-Log-Format finden Sie imMariaDB Server-Dokumentation.

DerAWS CloudAudit-Trail für IhreAWSDas Konto wird bereitgestellt von derAWS CloudTrailService. CloudTrailerfasst API-Aufrufe für Amazon RDS als Ereignisse. Alle Amazon RDS-Aktionen werden protokolliert. CloudTrailstellt eine Aufzeichnung der Aktionen in Amazon RDS bereit, die von einem Benutzer, einer Rolle oder einer anderen Person ausgeführt wurdenAWSService. Zu den Veranstaltungen gehören Maßnahmen, die in derAWSVerwaltungskonsole,AWS CLI, undAWSSDKs und APIs.

## Beispiel

In einem typischen Audit-Szenario müssen Sie möglicherweise Folgendes kombinierenAWS CloudTrailprotokolliert mit dem Datenbank-Audit-Log und der Amazon RDS-Ereignisüberwachung. Sie könnten beispielsweise ein Szenario haben, in dem die Datenbankparameter Ihrer Amazon RDS-DB-Instance (zum Beispiel`database-1`) wurden geändert und Ihre Aufgabe besteht darin, festzustellen, wer die Änderung vorgenommen hat, was geändert wurde und wann die Änderung stattgefunden hat.

Gehen Sie folgendermaßen vor, um die Aufgabe zu erledigen:

1. Listet die Amazon RDS-Ereignisse auf, die mit der Datenbank-Instance passiert sind`database-1`und stellen Sie fest, ob es ein Ereignis in der Kategorie gibt`configuration change`das hat die Botschaft`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. Identifizieren Sie, welche DB-Parametergruppe die DB-Instance verwendet:

```
$ 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. Benutze dieAWS CLIum zu suchenCloudTrailVeranstaltungenin der Region wo`database-1`wird in dem Zeitraum rund um das in Schritt 1 entdeckte Amazon RDS-Ereignis bereitgestellt und wo`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"
}
```

DerCloudTrailDie Veranstaltung zeigt, dass`User1`mit Rolle`Role1`vonAWSKonto 111122223333 hat die DB-Parametergruppe geändert`mariadb10-6-test`, das von der DB-Instance verwendet wurde`database-1`auf`2022-12-01 at 09:18:19 h`. Zwei Parameter wurden geändert und auf die folgenden Werte gesetzt:

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

## Zusätzliche CloudTrail und CloudWatch Funktionen protokollieren

Sie können Betriebs- und Sicherheitsvorfälle der letzten 90 Tage beheben, indem SieHistorie des Ereignissesauf derCloudTrailKonsole. Um den Aufbewahrungszeitraum zu verlängern und zusätzliche Abfragefunktionen zu nutzen, können SieAWS CloudTrailSee. MitAWS CloudTrailLake, Sie können Eventdaten bis zu sieben Jahre lang in einem Eventdatenspeicher aufbewahren. Darüber hinaus unterstützt der Dienst komplexe SQL-Abfragen, die eine umfassendere und anpassbarere Ansicht der Ereignisse bieten als die Ansichten, die durch einfache Suchvorgänge nach Schlüsselwerten inHistorie des Ereignisses.

Um Ihre Prüfprotokolle zu überwachen, Alarme einzurichten und Benachrichtigungen zu erhalten, wenn bestimmte Aktivitäten stattfinden, müssen Siekonfigurieren CloudTrailum seine Trailaufzeichnungen zu senden anCloudWatchLogs. Nach dem Trail werden die Aufzeichnungen gespeichert alsCloudWatchIn Protokollen können Sie Metrikfilter definieren, um Protokollereignisse anhand von Begriffen, Ausdrücken oder Werten auszuwerten, und Metrikfiltern Metriken zuweisen. Darüber hinaus können Sie erstellenCloudWatchAlarme, die gemäß den von Ihnen angegebenen Schwellenwerten und Zeiträumen generiert werden. Sie können beispielsweise Alarme konfigurieren,

die Benachrichtigungen an die zuständigen Teams senden, damit diese die entsprechenden Maßnahmen ergreifen können. Sie können CloudWatch auch so konfigurieren, dass als Reaktion auf einen Alarm automatisch eine Aktion durchgeführt wird.

# Warnfunktion

Benachrichtigungen sind eine der wichtigsten Informationsquellen, wenn es um die Sicherheit, Verfügbarkeit, Leistung und Zuverlässigkeit Ihrer IT-Infrastruktur und IT-Services geht. Sie benachrichtigen und informieren Ihre IT-Teams über anhaltende Sicherheitsbedrohungen, Ausfälle, Leistungsprobleme oder Systemausfälle.

Die Information Technology Infrastructure Library (ITIL), insbesondere die IT-Servicemanagement-Praktiken (ITSM), stellt automatische Warnmeldungen in den Mittelpunkt der Überwachung und des Eventmanagements sowie der Best Practices für das Incident-Management.

Beim Incident-Alerting generieren Monitoring-Tools Warnmeldungen, um Ihr Team zu informieren, und automatisierte Tools (für Elemente, die automatisch umsetzbar sind) über Änderungen, risikoreiche Aktionen oder Ausfälle in der IT-Umgebung. IT-Warnmeldungen sind die erste Verteidigungslinie gegen Systemausfälle oder Änderungen, die zu schwerwiegenden Vorfällen führen können. Durch die automatische Überwachung von Systemen und die Generierung von Warnmeldungen bei Ausfällen und riskanten Änderungen können IT-Teams Ausfallzeiten minimieren und die damit verbundenen hohen Kosten reduzieren.

Als bewährte Verfahren gelten dieAWSWell-Architected Framework schreibt vor, dass SieVerwenden Sie die Überwachung, um alarmbasierte Benachrichtigungen zu generieren, undproaktiv überwachen und alarmieren. BenutzenCloudWatchoder ein Überwachungsdienst eines Drittanbieters, der Alarme auslöst, die anzeigen, wenn die Messwerte außerhalb der erwarteten Grenzen liegen.

Der Zweck des Alarmmanagements besteht darin, effiziente, standardisierte Verfahren für den Umgang mit IT-bezogenen Ereignissen und Vorfällen festzulegen, indem Aktivitäten protokolliert, klassifiziert, Maßnahmen definiert und umgesetzt, abgeschlossen und nach einem Vorfall überprüft werden.

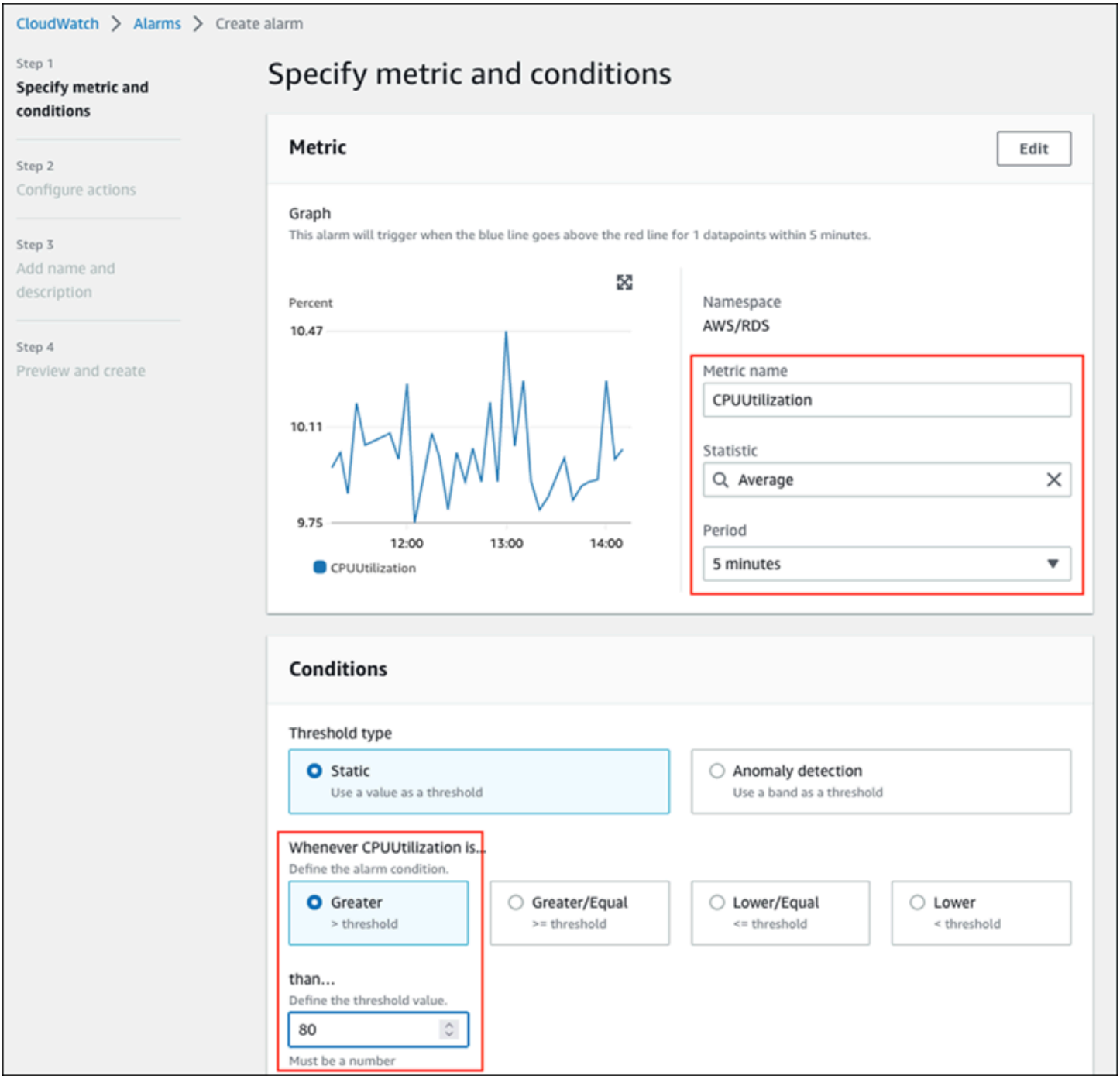
Sektionen

- CloudWatchAlarme
- EventBridgeRegeln
- Aktionen angeben, Alarme aktivieren und deaktivieren

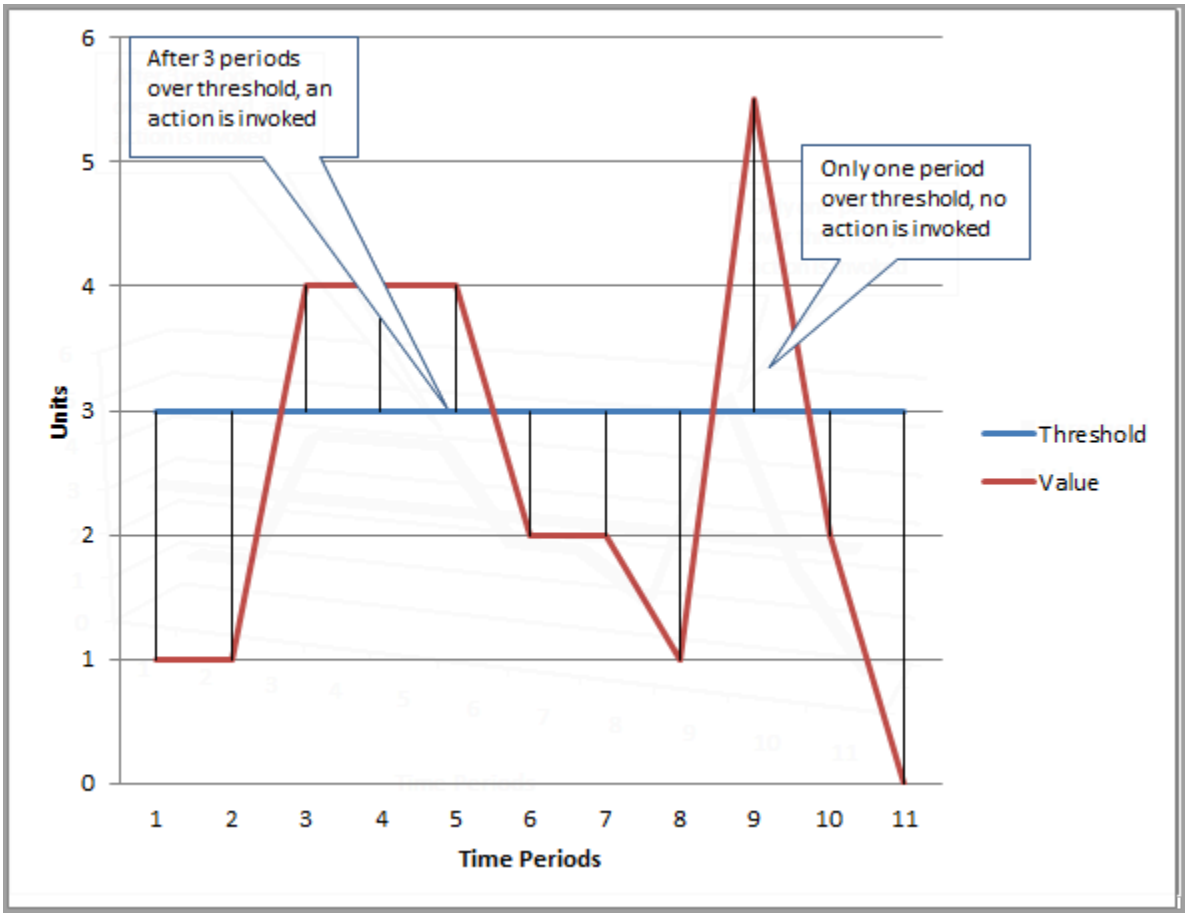
# CloudWatch-Alarme

Wenn Sie Ihre Amazon RDS-DB-Instances betreiben, möchten Sie verschiedene Arten von Metriken, Ereignissen und Traces überwachen und Warnmeldungen generieren. Für MySQL- und MariaDB-Datenbanken sind die kritischen InformationsquellenDB-Instance-Metriken,Betriebssystemmetriken,Ereignisse, Protokolle und Prüfprotokolle. Wir empfehlen Ihnen,CloudWatchAlarmeum eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum zu beobachten.

Das folgende Beispiel zeigt, wie Sie einen Alarm einrichten können, der die`CPUUtilization`Metrik (Prozentsatz der CPU-Auslastung) auf all Ihren Amazon RDS-DB-Instances. Sie konfigurieren den Alarm so, dass er ausgelöst wird, wenn die CPU-Auslastung auf einer DB-Instance während des Evaluierungszeitraums von 5 Minuten mehr als 80 Prozent beträgt.




Das bedeutet, dass der Alarm in die`ALARM`geben Sie an, ob eine Ihrer Datenbanken 5 Minuten oder länger eine hohe CPU-Auslastung (über 80 Prozent) aufweist. Der Alarm bleibt in der`OK`gibt an, ob die CPU gelegentlich für einen kurzen Zeitraum eine Auslastung von über 80 Prozent erreicht und dann wieder unter den Schwellenwert fällt. Die folgende Grafik veranschaulicht diese Logik.




CloudWatchAlarme unterstützen metrische und zusammengesetzte Alarme.

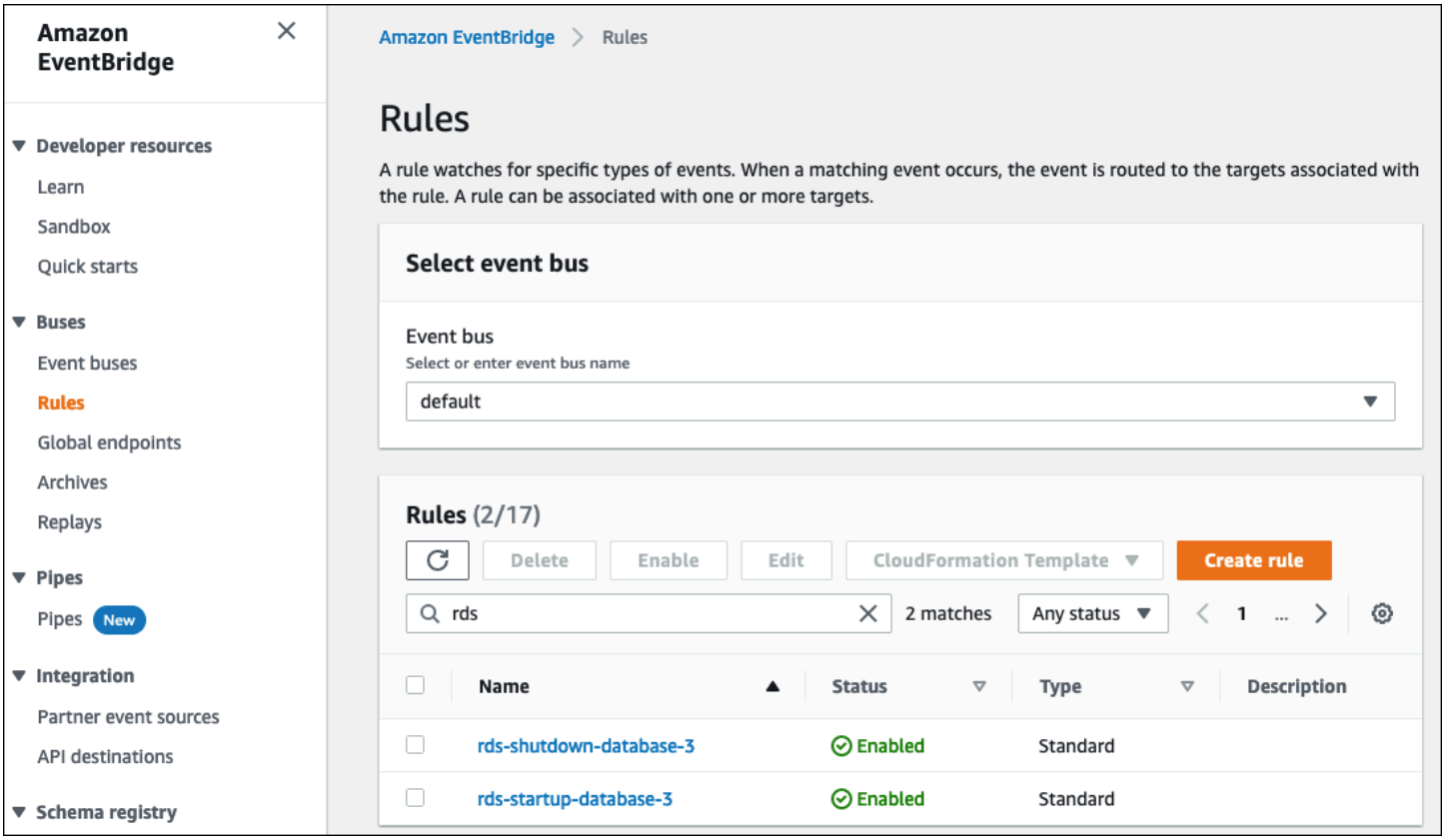
- EINmetrischer Alarmschaut sich eine Single anCloudWatchmetrisch und kann mathematische Ausdrücke für die Metrik ausführen. Ein metrischer Alarm kann Amazon SNS-Nachrichten senden, die wiederum auf der Grundlage des Werts der Metrik relativ zu einem bestimmten Schwellenwert über mehrere Zeiträume eine oder mehrere Aktionen ausführen können.
- EINzusammengesetzter Alarmbasiert auf einem Regelausdruck, der die Zustände mehrerer Alarme auswertet und in die`ALARM`nur angeben, wenn alle Bedingungen der Regel erfüllt sind. Verbundalarme werden in der Regel verwendet, um die Anzahl unnötiger Alarme zu reduzieren. Sie könnten beispielsweise einen zusammengesetzten Alarm haben, der mehrere metrische Alarme enthält, die so konfiguriert sind, dass sie niemals Aktionen ausführen. Der zusammengesetzte Alarm würde eine Warnung senden, wenn sich alle einzelnen metrischen Alarme im Composite bereits im`ALARM`

CloudWatchAlarme können nur zuschauenCloudWatchMetriken. Wenn Sie einen Alarm auf der Grundlage des Fehlers, einer langsamen Abfrage oder allgemeiner Protokolle

erstellen möchten, müssen SieCloudWatchMetriken aus den Protokollen. Sie können dies erreichen, wie bereits zuvor in derBetriebssystemüberwachungundEreignisse, Protokolle und PrüfprotokolleAbschnitte, indem Sie Filter verwenden, umMetriken aus Protokollereignissen erstellen. In ähnlicher Weise müssen Sie Metrikfilter in Bezug auf Kennzahlen von Enhanced Monitoring erstellenCloudWatchvonCloudWatchProtokolle.

## EventBridge-Regeln

Amazon RDS-Ereignissewerden an Amazon geliefertEventBridge, und du kannst benutzenEventBridgeRegelnum auf diese Ereignisse zu reagieren. Sie können zum Beispiel erstellenEventBridgeRegeln, die Sie benachrichtigen und Maßnahmen ergreifen würden, wenn eine bestimmte DB-Instance angehalten oder gestartet wird, wie der folgende Bildschirm zeigt.

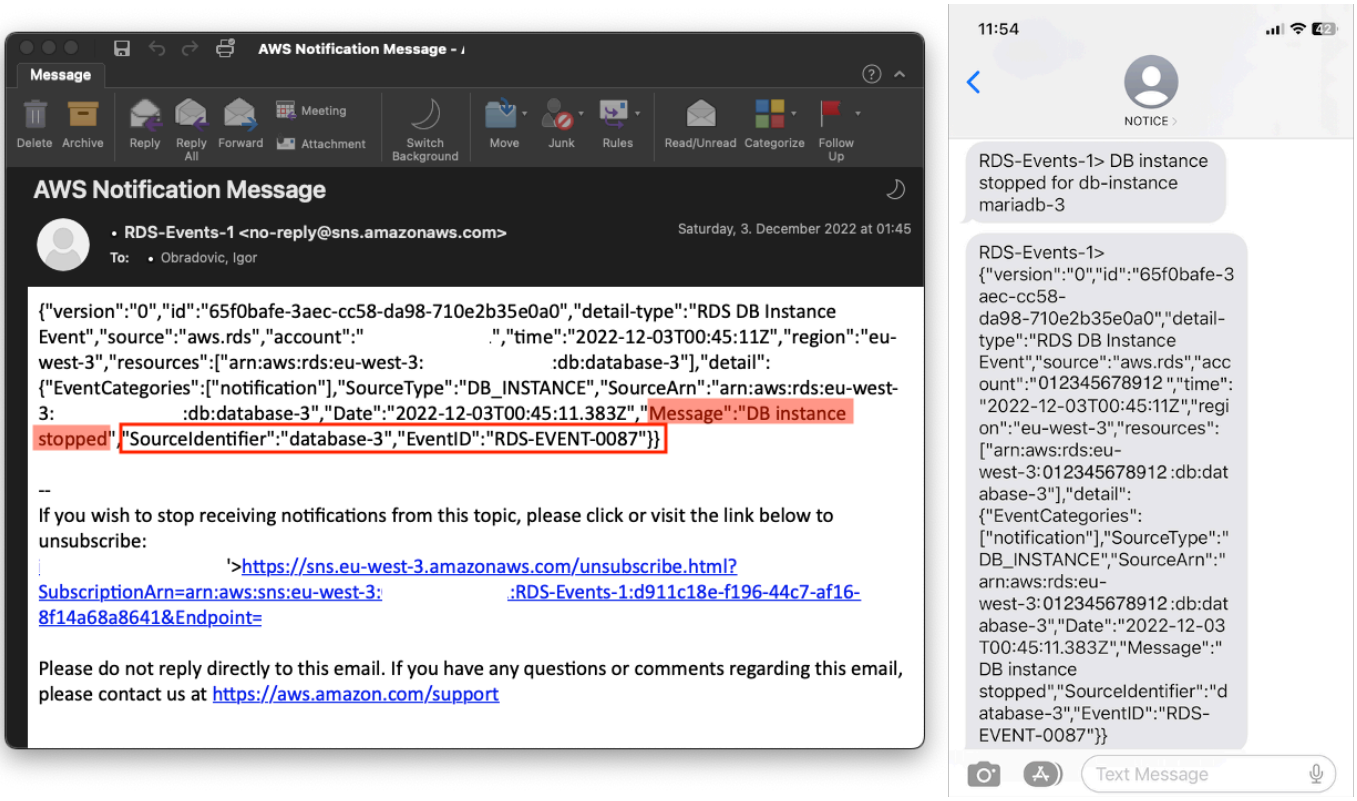



Die Regel, die erkenntThe `DB instance has been stopped`Ereignis hat die Amazon RDS-Event-ID`RDS-EVENT-0087`, also stellst du die`Event Pattern`Eigentum der Regel an:

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

Diese Regel überwacht die DB-Instance`database-3`nur, und achtet auf die`RDS-EVENT-0087`Ereignis. WannEventBridgeerkennt das Ereignis und sendet es an eine Ressource oder einen Endpunkt, bekannt alsZiel. Hier können Sie die Aktion angeben, die Sie ergreifen möchten, wenn die Amazon RDS-Instance heruntergefahren wird. Sie können das Ereignis an viele mögliche Ziele senden, darunter ein SNS-Thema, eine Amazon Simple Queue Service (Amazon SQS) -Warteschlange, eineAWS Lambdafunktion,AWS Systems ManagerAutomatisierung, einAWS BatchJob, Amazon API Gateway, ein Reaktionsplan im Incident Manager, eine Funktion vonAWS Systems Managerund viele andere. Sie können beispielsweise ein SNS-Thema erstellen, das eine Benachrichtigungs-E-Mail und eine SMS sendet, und dieses SNS-Thema als Ziel für dieEventBridgeRegel. Wenn die Amazon RDS-DB-Instance`database-3`wurde gestoppt, Amazon RDS liefert das Ereignis`RDS-EVENT-0087`zuEventBridge, wo es erkannt wird. EventBridgeruft dann das Ziel auf, was das SNS-Thema ist. Das SNS-Thema ist so konfiguriert, dass es eine E-Mail (wie in der folgenden Abbildung gezeigt) und eine SMS sendet.



# Aktionen angeben, Alarme aktivieren und deaktivieren

Sie können eine verwendenCloudWatchAlarm, um anzugeben, welche Aktionen der Alarm ergreifen soll, wenn er zwischen`OK`,`ALARM`, und`INSUFFICIENT_DATA`Staaten. CloudWatchverfügt über eine integrierte Integration mit SNS-Themen und mehreren zusätzlichen Aktionskategorien, die nicht für Amazon RDS-Metriken gelten, wie Amazon Elastic Compute Cloud (Amazon EC2) -Aktionen oder Amazon EC2 Auto Scaling-Gruppenaktionen. EventBridgewird im Allgemeinen verwendet, um Regeln zu schreiben und Ziele zu definieren, die Maßnahmen ergreifen, wenn der Alarm für Amazon RDS-Metriken ausgelöst wird. CloudWatchsendet Ereignisse anEventBridgejedes Mal einCloudWatchAlarm ändert seinen Zustand. Sie können diese Ereignisse zur Änderung des Alarmzustands verwenden, um ein Ereignisziel in auszulösenEventBridge. Weitere Informationen finden Sie unterAlarmereignisse undEventBridgein derCloudWatchdokumentation.

Möglicherweise müssen Sie auch Alarme verwalten, z. B. um einen Alarm bei geplanten Konfigurationsänderungen oder Tests automatisch zu deaktivieren und den Alarm dann wieder zu aktivieren, wenn die geplante Aktion abgeschlossen ist. Wenn Sie beispielsweise ein geplantes, geplantes Upgrade der Datenbanksoftware haben, das Ausfallzeiten erfordert, und Sie über Alarme verfügen, die aktiviert werden, wenn die Datenbank nicht verfügbar ist, können Sie Alarme mithilfe der API-Aktionen deaktivieren und aktivierenDisableAlarmActionsundEnableAlarmActions, oder diedisable-alarm-actionsundenable-alarm-actionsBefehle in derAWS CLI. Sie können den Verlauf des Alarms auch auf derCloudWatchKonsole oder mit derDescribeAlarmHistoryAPI-Aktion oder diedescribe-alarm-historyBefehl in derAWS CLI. CloudWatch speichert den Alarmverlauf zwei Wochen lang. Auf derCloudWatchKonsole, du kannst die wählenFavoriten und aktuelleMenü im Navigationsbereich, um Ihre bevorzugten und zuletzt besuchten Alarme einzustellen und darauf zuzugreifen.

# Nächste Schritte und Ressourcen

Weitere Informationen zur Migration Ihrer relationalen Datenbanken zu denAWS Cloud, siehe die folgende Strategie auf derAWSWebsite zur präskriptiven Beratung:

- Migrationsstrategie für relationale Datenbanken

Du kannst erkundenMuster der Datenbankmigrationzumstep-by-stepAnweisungen zu Ihren spezifischen relationalen Datenbanken, die in der laufenAWS Cloud, einschließlich Aufgaben im Zusammenhang mit Überwachung, Migration und Datenmanagement.

Verwenden Sie die Filter auf dieser Seite, um Muster zu finden nachAWSService (z. B. Migrationen zu Amazon RDS oder Amazon Aurora), nach Arbeitslast (z. B. Open Source, einschließlich MySQL- und MariaDB-Datenbanken) oder nach geplanter Nutzung (Produktion oder Pilotprojekt).

Weitere Ressourcen finden Sie im Folgenden:

- Amazon Relational Database Service-Benutzerhandbuch
- AmazonasCloudWatchBenutzerleitfaden
- Häufig gestellte Fragen zu Amazon RDS
- Häufig gestellte Fragen zu Performance Insights
- Stellen Sie mithilfe von Amazon RDS Performance Insights Zählerkennzahlen an einen Drittanbieter zur Überwachung der Anwendungsleistung bereitCloudWatchStream mit Metriken(AWSBlogbeitrag)
- Ein Amazon erstellenCloudWatchDashboard zur Überwachung von Amazon RDS und Amazon Aurora MySQL(AWSBlogbeitrag)
- Optimierung von Amazon RDS für MySQL mit Performance Insights(AWSBlogbeitrag)

# Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| Die Informationen wurden aktualisiert | Die Informationen über Exporteure wurden aktualisiert und Richtlinien für die Auswahl eines Exporteurs hinzugefügt. | 13. Juni 2024 |
| Erste Veröffentlichung | — | 30. Juni 2023 |

# AWS Glossar zu präskriptiven Leitlinien

Im Folgenden finden Sie häufig verwendete Begriffe in Strategien, Leitfäden und Mustern, die von Prescriptive Guidance bereitgestellt AWS werden. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

## Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Faktorwechsel/Architekturwechsel – Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile cloudnativer Feature nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre On-Premises-Oracle-Datenbank zu der PostgreSQL-kompatible Amazon-Aurora-Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der AWS Cloud.
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr CRM-System (Customer Relationship Management) zu Salesforce.com.
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf einer EC2-Instance in der Cloud zu Oracle. AWS
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Dieses Migrationsszenario ist spezifisch für VMware Cloud on AWS, das die Kompatibilität mit virtuellen Maschinen (VM) und die Workload-Portabilität zwischen Ihrer lokalen Umgebung und unterstützt. AWS Sie können die VMware-Cloud-Foundation-Technologien von Ihren On-Premises-Rechenzentren aus verwenden, wenn Sie

Ihre Infrastruktur zu VMware Cloud in AWS migrieren. Beispiel: Verlagern Sie den Hypervisor, der Ihre Oracle-Datenbank hostet, zu VMware Cloud on. AWS

- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.
- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

# A

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank Transaktionen von verbindenden Anwendungen verarbeitet, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung von AIOps in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Betriebsintegration.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Einführung der Cloud (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt. AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und

Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

# B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser

E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

Blau/Grün-Bereitstellung

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, sogenannte bösartige Bots, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den

er in der Regel keine Zugriffsrechte besitzt. Weitere Informationen finden Sie unter dem Indikator Implementation break-glass procedures in den AWS Well-Architected-Leitlinien.

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

# C

CAF

Weitere Informationen finden Sie unter Framework für die AWS Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen normalerweise durchlaufen, wenn sie zur AWS Cloud migrieren:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Neuentwicklung – Optimierung von Produkten und Services und Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oder AWS CodeCommit. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD-Pipeline kann mehrere Repositorien verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. AWS Panorama Bietet beispielsweise Geräte an, die CV zu lokalen Kameranetzwerken hinzufügen, und Amazon SageMaker stellt Bildverarbeitungsalgorithmen für CV bereit.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

Kontinuierliche Bereitstellung und kontinuierliche Integration (CI/CD)

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD wird allgemein als Pipeline beschrieben. CI/CD kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere

Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

# D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil der Sicherheitssäule im AWS Well-Architected Framework. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, mit denen sichergestellt werden kann, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen historischer Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

defense-in-depth

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein defense-in-depth Ansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren AWS Organizations, um die Konten der Organisation zu verwalten und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Bereitstellung

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, mit denen Sie Ausfallzeiten und Datenverluste aufgrund einer Katastrophe minimieren. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domaingesteuertes

Design: Bewältigen der Komplexität im Herzen der Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domaingesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung der Wertströme in der Entwicklung.

# E

EDA

Siehe explorative Datenanalyse.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-Endian-Systeme speichern das höchstwertige Byte zuerst. Little-Endian-Systeme speichern das niedrigwertigste Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.
- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.

- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD-Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsthemen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS - Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

# F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit:AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

# G

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub, Amazon

GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

# H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, eine gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

## I

IaC

Sehen Sie Infrastruktur als Code.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im AWS Well-Architected Framework.

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und KI/ML bezieht.

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

Industrielles Internet der Dinge (IIoT)

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Mehr Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in derselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für Machine Learning mit AWS.

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

# L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

Große Migration

Eine Migration von 300 oder mehr Servern.

SCHWARZ

Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

Niedrigere Umgebungen

Siehe Umwelt.

# M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Nachverfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Aufbau von Mechanismen im AWS Well-Architected Framework.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind. AWS Organizations Ein Konto kann jeweils nur einer Organisation angehören.

DURCHEINANDER

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes machine-to-machine (M2M) -Kommunikationsprotokoll, das auf dem Publish/Subscribe-Muster für IoT-Geräte mit beschränkten Ressourcen basiert.

Microservice

Ein kleiner, unabhängiger Service, der über klar definierte APIs kommuniziert und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren über eine klar definierte Schnittstelle mithilfe einfacher APIs. Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementieren von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Funktionsübergreifende Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams in der Migrationsabteilung gehören in der Regel Betriebsabläufe, Geschäftsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration in die Cloud bereitstellt. AWS MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wird, um einen Workload in die AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um groß angelegte Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Bewertung der Modernisierungsbereitschaft von Anwendungen in der AWS -Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Für eine verbesserte Konsistenz, Zuverlässigkeit und Vorhersagbarkeit empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

# O

OAC

Siehe Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein machine-to-machine (M2M) -Kommunikationsprotokoll für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren. Weitere Informationen finden Sie unter Operational Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Einen Trail für eine Organisation erstellen.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische `PUT` und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ODER

Siehe Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

# P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht. Weitere Informationen finden Sie unter Datenpersistenz in Microservices aktivieren.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder

einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz durch Design

Ein Ansatz in der Systemtechnik, der den Datenschutz während des gesamten Engineering-Prozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Diese Steuerelemente scannen Ressourcen, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

veröffentlichen/abonnieren (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

# Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

# R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Dies bestimmt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Betriebsunterbrechung angesehen wird.

Ziel der Wiederherstellungszeit (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten für alle Parteien definiert, die an Migrationsaktivitäten und Cloud-Vorgängen beteiligt sind. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel der Wiederherstellungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

# S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS Management Console oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Secret in der Secrets Manager-Dokumentation.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

: Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPs definieren Integritätsschutz oder legen Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Services oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

: Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

: Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

: Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

: Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

: Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, wohingegen Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

SIEM

: Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

: Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

split-and-seed Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der AWS Cloud.

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweises Modernisieren älterer Microsoft ASP.NET (ASMX)-Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

# T

tags

Schlüssel-Wert-Paare, die als Metadaten für die Organisation Ihrer Ressourcen dienen. AWS Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

Transit-Gateway

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der AWS Transit Gateway Dokumentation unter Was ist ein Transit-Gateway.

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

# U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt. Weitere Informationen finden Sie im Leitfaden Quantifizieren der Unsicherheit in Deep-Learning-Systemen.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

# V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs, mit der Sie den Datenverkehr mithilfe von privaten IP-Adressen weiterleiten können. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems gefährdet.

# W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Mal schreiben, viele lesen.

WQF

Weitere Informationen finden Sie unter AWS Workload Qualification Framework.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur wird als unveränderlich angesehen.

# Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.