适用于 MySQL 的 Amazon RDS 和 MariaDB 的监控和警报工具以及最佳实践

AWS 规范性指导

AWS 规范性指导: 适用于 MySQL 的 Amazon RDS 和 MariaDB 的监控和警报工具以及最佳实践

Table of Contents

适用于 MySQL 和 MariaDB 的 Amazon RDS 的监控和警报工具及最佳实践

伊戈尔·奥布拉多维奇，亚马逊网络服务（AWS）

2023 年 6 月（文档历史）

数据库监控是测量、跟踪和评估数据库可用性、性能和功能的过程。监控和警报解决方案可帮助组织确保其数据库服务以及相关的应用程序和工作负载安全、高性能、弹性和高效。在 AWS 上，您可以收集和分析工作负载日志、指标、事件和跟踪，以了解工作负载的运行状况，并从一段时间内的操作中获得见解。

您可以监控您的资源以确保它们按预期运行，并在任何问题影响您的客户之前检测和修复。当阈值被突破时，您应该使用监控的指标、日志、事件和跟踪来发出警报。

本指南介绍了 Amazon 关系数据库服务 (Amazon RDS) 数据库的数据库可观测性和监控工具以及最佳实践。该指南侧重于 MySQL 和 MariaDB 数据库，尽管大多数信息也适用于其他 Amazon RDS 数据库引擎。

本指南适用于解决方案架构师、数据库架构师、DBA 和资深人士DevOps参与为 AWS 云中运行的数据库工作负载设计、实施和管理监控和可观测性解决方案的工程师和其他团队成员。

内容

概述

监控和警报包含在 Well-Ar AWS chitected Framework 的四个支柱中。

- 卓越运营支柱规定，您的工作负载设计应包括遥测和监控。 AWS 诸如 Amazon Relational Database Service (Amazon RDS) 之类的服务可为您提供了解工作负载内部状态所必需的信息（例如，指标、日志、事件和跟踪）。在操作 Amazon RDS 数据库时，您需要了解数据库实例的运行状况，检测操作事件，并能够对计划内和计划外事件做出响应。AWS 提供的监控工具可帮助您确定组织和业务成果何时面临风险或可能面临风险，以便您能够在正确的时间采取适当的措施。
- 性能效率支柱规定，您应通过实时收集、汇总和处理与性能相关的指标来监控资源（例如 Amazon RDS 数据库实例）的性能。您可以识别性能下降并修复导致性能下降的因素，例如 SQL 查询未优化或配置参数不足。当测量值超出预期边界时，您可以自动发出警报。我们建议您不仅要使用警报来发送通知，还要针对检测到的事件启动自动操作。您可以根据预定义的阈值评估收集的指标，也可以使用机器学习算法来识别异常行为。例如，要检测 CPU 利用率增加的趋势，您可以收集和分析一段时间内的`cpuUtilization.total`指标。在 CPU 利用率达到硬限制之前主动提醒该异常情况，可以帮助您在问题影响客户之前对其进行修复。
- 可靠性支柱将监控和警报定义为确保您满足可用性要求的关键。您的监控解决方案必须能够有效地检测故障。当它检测到问题或故障时，其主要目标是对这些问题发出警报。对于云端的弹性架构而言，实施持续的可观察性和监控实践是当务之急。要改善您的工作负载，您必须能够对其进行衡量并了解其状态和运行状况。自动从故障中恢复、横向扩展和容量配置的设计原则取决于准确的监控和警报服务。
- 安全支柱讨论了检测和预防意外或不必要的配置更改以及意外行为。您可以使用 MariaDB 审计插件配置适用于 MySQL 的 Amazon RDS 和 Maria DB 数据库实例，以记录数据库活动，例如用户登录和针对数据库运行的特定操作。该插件将数据库活动记录存储在日志文件中，该文件可以集成并导入到监控和警报工具中。对日志文件进行实时分析，以确定数据库中是否存在意外或可疑行为。此类意外或可疑行为可能表明您的 Amazon RDS 数据库实例已遭到入侵，这表明您的业务面临潜在风险。如果监控工具检测到此类事件，则会激活警报以启动对安全事件的响应，这有助于解决可疑和恶意活动。

目标业务成果

在监控和警报机制中实施最佳实践可帮助您确保为应用程序和工作负载提供高性能、弹性、高效、安全且成本优化的基础架构。您可以使用可观察性工具来实时收集、存储和可视化指标、事件、跟踪和日志，以观察和分析数据库的运行状况和性能的大局，从而防止关联的 IT 服务降级或中断。如果仍出现

计划外降级或服务中断，则监控和警报工具可帮助您及时检测问题、上报、做出反应，以及快速调查和解决问题。针对云数据库工作负载的全面监控和警报解决方案可帮助您实现以下业务成果：

- 改善客户体验。可靠的服务可以改善您的客户体验。数据库通常是数字服务的关键组成部分，例如网络和移动应用程序、媒体流、支付、 business-to-business (B2B) API 和集成服务。如果您能够在数据库上监控和设置警报以快速检测问题，高效地调查问题，并尽快修复问题，从而最大限度地减少停机时间和其他中断，那么您就可以为客户增强数字服务的可用性、安全性和性能。
- 建立客户信任。更好的性能和更流畅的用户体验可以帮助您赢得客户的信任，从而在您的平台上带来更多业务。例如，提供可靠在线服务的支付处理服务提供商可以期望获得较高的客户信任度和忠诚度，从而带来更多的客户和更好的留存率，增加可计费的交易，以及创造更多收入的新型创新服务。
- 避免经济损失。数据库基础架构中的任何意外停机都可能影响客户使用您的应用程序执行的业务事务。在某些情况下，这可能会导致重大的经济损失。违反服务级别协议 (SLA) 可能会导致客户失去信任，从而导致收入损失。它也可以成为昂贵试验的法律依据，在这种试验中，客户可能会根据您的责任和保修合同要求赔偿。根据软件公司 Atlassian Corporation的一项研究，服务中断的平均成本在每小时14万至5.4万美元之间，具体取决于业务的类型和规模。稳定的数据库环境是防止长时间中断和业务损失的关键。
- 扩大价值。监控和警报机制可以帮助您设计、开发和运营高可用性、弹性、可靠、高性能、经济实惠且安全的数字服务，但这仅仅是个开始。随着时间的推移，您会希望您的组织能够扩展并蓬勃发展，增强现有的云工作负载，并引入新的服务。新服务可为您的客户提供额外价值，为您的业务带来更多收入，从而对您的业务增长产生飞轮效应。
- 提高开发人员的工作效率。高效、高效且在开发任务中没有遇到问题和瓶颈的开发人员可以在更短的时间内交付高质量的产品。但是，软件工程和 IT 运营往往面临复杂的挑战，这种复杂性会随着工作负载及其架构的规模而增加。要分析分布式应用程序的性能和一致性，开发人员需要能够提供相关指标和跟踪的工具。它们有助于尽快识别有缺陷的代码工件和基础架构组件，并有助于确定对最终用户的影响。合适的监控和警报工具套件可以帮助开发人员更好、更快地进行编码和测试。
- 提高运营效率和效率。当您大规模操作云工作负载时，即使是一小部分性能改进也可以节省数百万美元。通过监控您的数据库并分析指标、事件、日志和跟踪，您可以了解和预测未来的容量需求，并可以利用 AWS 云中提供的成本节约。了解您的 Amazon RDS 工作负载和运行状况可以帮助您应对事件、修复问题和计划改进。

一般最佳实践

以下最佳实践可帮助您充分了解 Amazon RDS 工作负载的运行状况，并采取适当的措施来响应操作事件和监控数据。

- 确定关键绩效指标。根据预期的业务成果确定关键绩效指标 (KPI)。评估 KPI 以确定工作负载是否成功。例如，如果您的核心业务是电子商务，那么您想要的业务成果之一可能是您的电子商店全天候可供客户购物。要实现该业务成果，您需要为您的电子商店应用程序使用的后端 Amazon RDS 数据库定义可用性 KPI，并将基准 KPI 设置为每周一次 99.99%。根据基准值评估实际可用性 KPI 可帮助您确定您是否满足所需的 99.99% 的数据库可用性，从而实现全天候服务的业务成果。
- 定义工作负载指标。定义工作负载指标以衡量您的 Amazon RDS 工作负载的数量和质量。评估指标以确定工作负载是否实现了预期的结果，并了解工作负载的运行状况。例如，要评估您的 Amazon RDS 数据库实例的可用性 KPI，您应该衡量数据库实例的正常运行时间和停机时间等指标。然后，您可以使用这些指标来计算可用性 KPI，如下所示：

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

  指标表示按时间顺序排列的数据点集。指标还可以包括维度，这在分类和分析中很有用。
- 收集和分析工作负载指标。Amazon RDS 会根据您的配置生成不同的指标和日志。其中一些代表数据库实例事件、计数器或统计数据，例如`db.Cache.innoDB_buffer_pool_hits`。其他指标来自操作系统，例如`memory.Total`，它衡量主机亚马逊弹性计算云 (Amazon EC2) 实例的总内存量。监控工具应对收集的指标进行定期、主动的分析，以确定趋势并确定是否需要任何适当的应对措施。
- 建立工作负载指标基准。为指标建立基线，以定义预期值并确定好坏阈值。例如，您可以为以下各项定义基线`ReadIOPS`在正常的数据库操作下最多可达 1,000。然后，您可以使用此基准进行比较并识别过度使用情况。如果您的新指标始终显示读取 IOPS 在 2,000-3,000 之间，则您已经发现了一个偏差，该偏差可能会触发调查、干预和改进的响应。
- 在工作负载结果面临风险时发出警报。当您确定业务结果存在风险时，请发出警报。然后，您可以在问题影响客户之前主动解决问题，也可以及时减轻事件的影响。
- 确定工作负载的预期活动模式。根据您的指标基准，建立工作负载活动模式以识别意外行为，并在必要时采取适当的措施进行响应。AWS提供监控工具它们应用统计和机器学习算法来分析指标和检测异常。
- 检测到工作负载异常时发出警报。在 Amazon RDS 工作负载的操作中检测到异常时，发出警报，以便在必要时采取适当的措施进行响应。

- 审查和修改 KPI 和指标。确认您的 Amazon RDS 数据库符合您定义的要求，并确定实现业务目标的潜在改进领域。验证测得的指标和评估的 KPI 的有效性，并在必要时对其进行修改。例如，假设您为最佳并发数据库连接数设置了 KPI，并监控有关尝试和失败的连接以及已创建和正在运行的用户线程的指标。您的数据库连接可能多于 KPI 基线定义的连接。通过分析当前的指标，您可以检测结果，但可能无法确定根本原因。如果是，则应修改指标并纳入其他监控措施，例如表锁计数器。新指标将有助于确定数据库连接数量的增加是否是由意外的表锁引起的。

监控工具

我们建议您使用可观察性、监控和警报工具来：

- 深入了解您的 Amazon RDS 环境的性能
- 检测意外和可疑行为
- 规划容量并就分配 Amazon RDS 实例做出明智的决定
- 分析指标和日志，主动预测潜在问题
- 在突破阈值时生成警报，以便在用户受到影响之前进行故障排除和解决

您可以选择不同的选项和解决方案，包括 AWS 提供的云原生可观察性和监控工具和服务；免费的开源软件解决方案；以及用于监控 Amazon RDS 数据库实例的商业第三方解决方案。以下各节将讨论其中一些工具。

要确定哪种工具最适合您的需求，请将每种工具的特性和功能与组织的要求进行比较。我们还建议您评估这些工具是否易于部署、配置和集成、软件更新和维护、部署方法（例如，硬件或无服务器）、许可、价格以及组织特定的任何其他因素。

Sections

亚马逊 RDS 中包含的工具

Amazon Relational Database Service（Amazon RDS）是 AWS 云中的一项托管数据库服务。由于 Amazon RDS 是一项托管服务，因此您可以从大多数管理任务中解放出来，例如数据库备份、操作系统 (OS) 和数据库软件安装、操作系统和软件修补、高可用性设置、硬件生命周期和数据中心操作。

AWS 还提供了一套全面的工具，使您能够为 Amazon RDS 数据库实例构建完整的可观察性解决方案。

一些监控工具已包含在 Amazon RDS 服务中，并已预先配置并自动启用。启动新的 Amazon RDS 实例后，您可以立即使用两个自动工具：

- Amazon RDS 实例状态提供有关数据库实例当前运行状况的详细信息。例如，状态代码包括 “可用”、“已停止”、“正在创建”、“正在备份” 和 “失败”。您可以使用 Amazon RDS 控制台、 AWS Command Line Interface (AWS CLI) 或 Amazon RDS API 来查看实例状态。有关更多信息，请参阅 Amazon RDS 文档中的查看 Amazon RDS 数据库实例状态。
- Amazon RDS 建议为数据库实例、只读副本和数据库参数组提供自动建议。这些建议是通过分析数据库实例使用情况、性能数据和配置来提供的，并作为指导提供。例如，引擎版本过时的建议表明您的数据库实例未运行最新版本的数据库软件，因此您应升级数据库实例以受益于最新的安全修复和其他改进。有关更多信息，请参阅亚马逊 RDS 文档中的查看 Amazon RDS 建议。

CloudWatch 命名空间

Amazon RDS 与 Amazon 集成 CloudWatch，后者是一项针对在 AWS 上运行的云资源和应用程序的监控和警报服务。Amazon RDS 会自动收集有关数据库实例的操作、利用率、性能和运行状况的指标、日志文件、跟踪和事件，并将其发送到以 CloudWatch 进行长期存储、分析和警报。

适用于 MySQL 的 Amazon RDS 和适用于 MariaDB 的 Amazon RDS 会在一分钟 CloudWatch内自动向其发布一组默认指标，无需额外付费。这些指标被收集到两个命名空间中，它们是指标的容器：

- AWS/RDS 命名空间包括数据库实例级别的指标。示例包括`BinLogDiskUsage`（二进制日志占用的磁盘空间量）、`CPUUtilization`（CPU 利用率的百分比）、`DatabaseConnections`（与数据库实例的客户端网络连接数）等等。
- AWS/Usage 命名空间包括账户级别的使用量指标，这些指标用于确定您是否在 A ma zon RDS 服务配额内进行操作。示例包括`DBInstances`（您的 AWS 账户或区域中的数据库实例数量）、`DBSubnetGroups`（您的 AWS 账户或区域中的数据库子网组数量）和`ManualSnapshots`（您的 AWS 账户或区域中手动创建的数据库快照数量）。

CloudWatch 按如下方式保留指标数据：

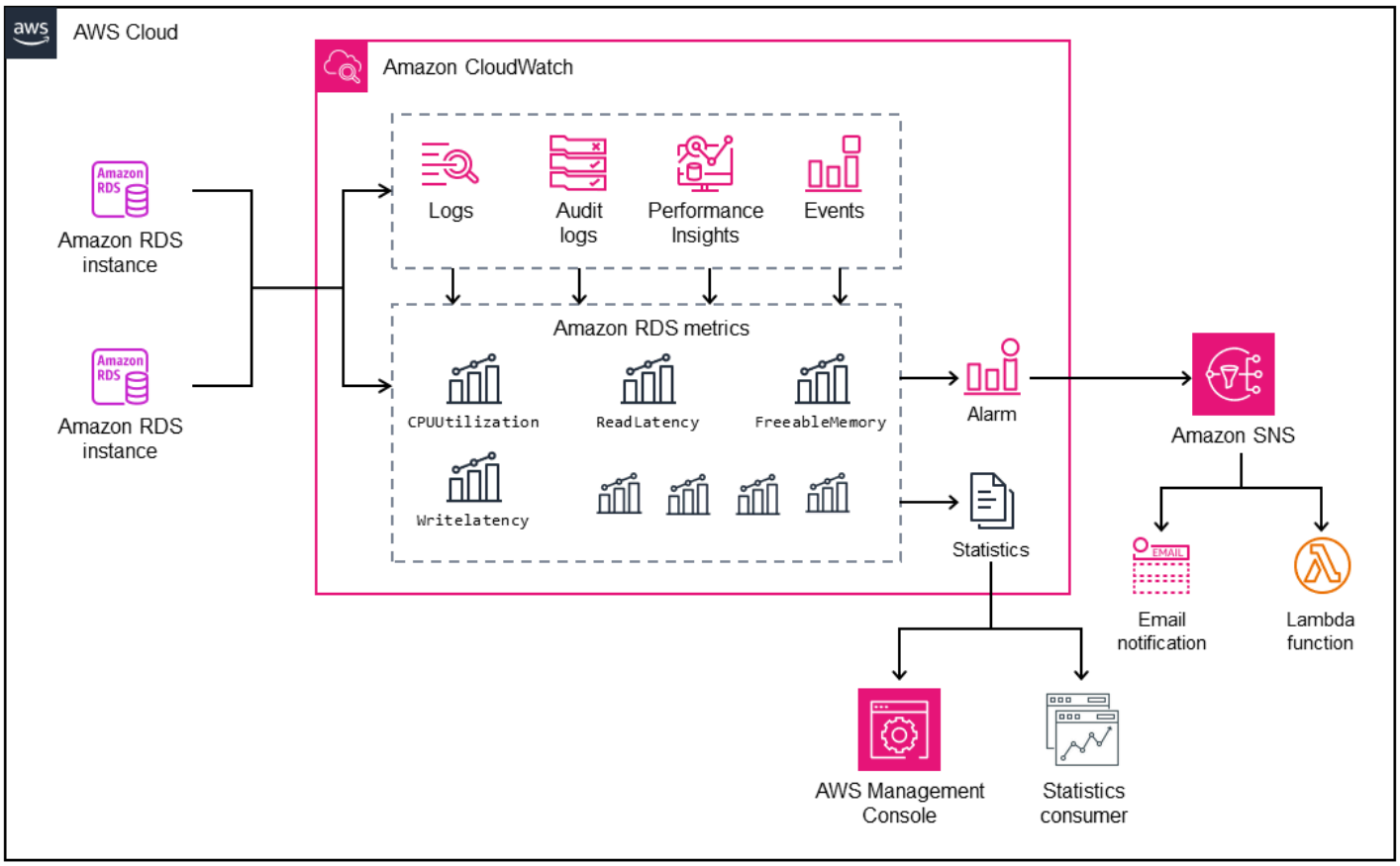
- 3 小时：时间小于 60 秒的高分辨率自定义指标将保留 3 小时。3 小时后，数据点将汇总为 1 分钟周期指标并保存 15 天。

- 15 天：周期为 60 秒（1 分钟）的数据点保留 15 天。15 天后，数据点将汇总为 5 分钟周期指标，并保存 63 天。
- 63 天：周期为 300 秒（5 分钟）的数据点保留 63 天。63 天后，数据点将汇总为 1 小时周期指标，并保存 15 个月。
- 15 个月：周期为 3,600 秒（1 小时）的数据点可用 15 个月（455 天）。

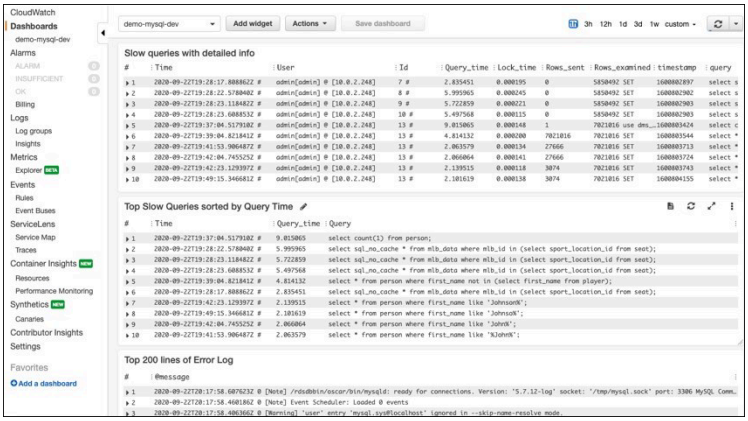
有关更多信息，请参阅 CloudWatch 文档中的指标。

CloudWatch 警报和仪表板

您可以使用 Amazon CloudWatch 警报在一段时间内监视特定的 Amazon RDS 指标。例如，您可以监控`FreeStorageSpace`指标的值是否超过您设置的阈值，然后执行一项或多项操作。如果您将阈值设置为 250 MB，且可用存储空间为 200 MB（小于阈值），则警报将被激活，并可能触发一项操作，自动为 Amazon RDS 数据库实例配置额外存储空间。警报还可以使用亚马逊简单通知服务 (Amazon SNS) Service 向数据库管理员发送通知短信。下图阐明了此过程。

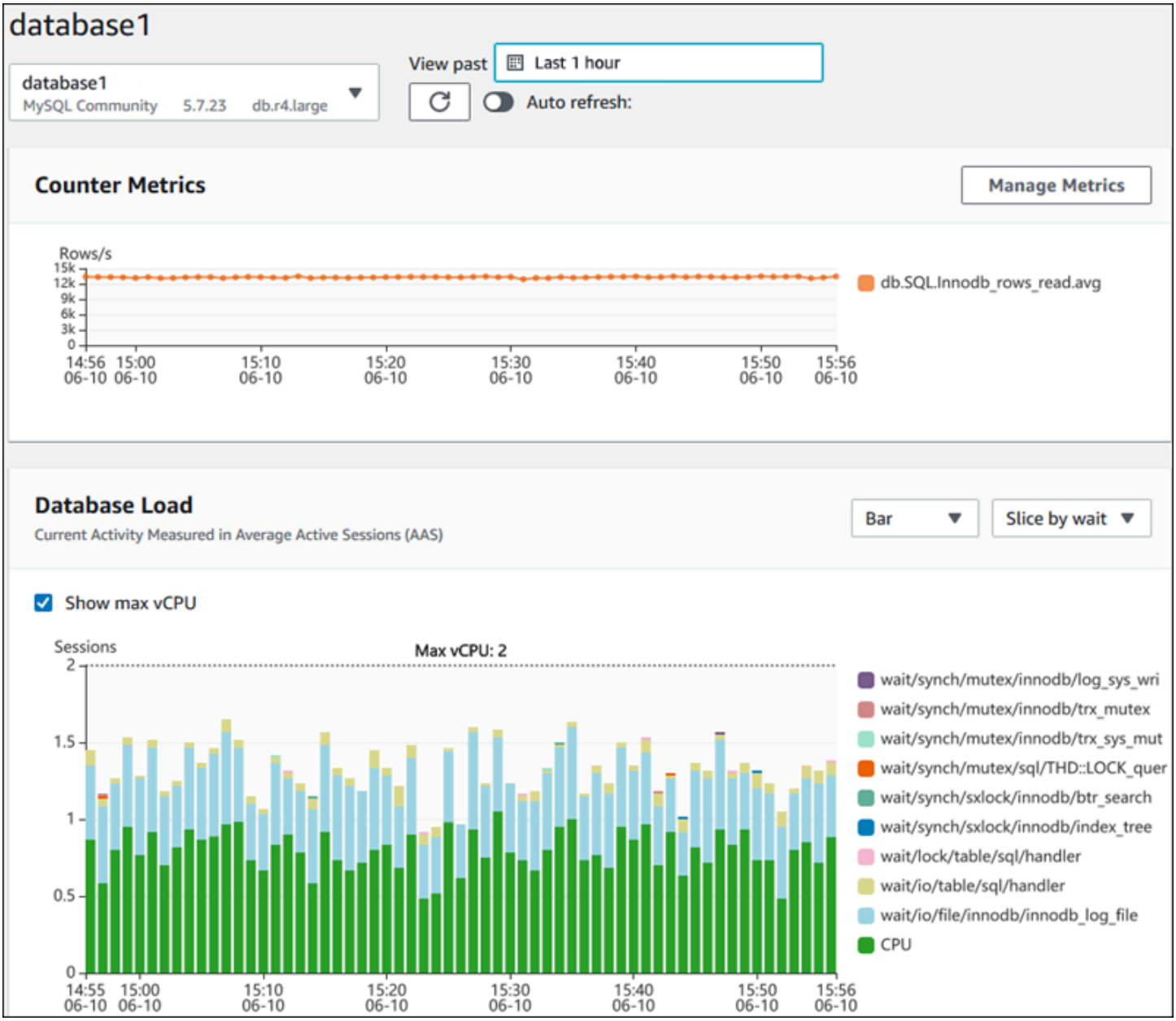


CloudWatch 还提供仪表板，可用于创建、自定义、与指标交互和保存自定义视图（图表）。您还可以使用 CloudWatch Logs Insights 创建仪表板，用于监控慢速查询日志和错误日志，并在这些日志中检测到特定模式时接收警报。以下屏幕显示了一个 CloudWatch仪表板示例。



Amazon RDS 性能详情

Amazon RDS Performance Insights 是一款数据库性能调整和监控工具，它扩展了 Amazon RDS 监控功能。它通过可视化数据库实例负载并按等待、SQL 语句、主机或用户筛选负载来帮助您分析数据库的性能。该工具将多个指标组合成一个交互式图表，可帮助您识别数据库实例可能存在的瓶颈类型，例如锁定等待、高 CPU 消耗或 I/O 延迟，并确定哪些 SQL 语句造成了瓶颈。以下屏幕显示了一个可视化示例。



您必须在数据库实例创建过程中启用 Performance Insigh ts，才能收集账户中的 Amazon RDS 数据库实例的指标。免费套餐包括七天的性能数据历史记录和每月一百万个 API 请求。或者，您可以购买更长的保留期。有关完整的定价信息，请参阅性能详情定价。

有关如何使用 Performance Insights 监控数据库实例的信息，请参阅本指南后面的数据库实例监控部分。

Performan ce Insights 自动向发布指标 CloudWatch。除了使用 Performance Insights 工具外，您还可以利用该工具 CloudWatch 提供的其他功能。您可以使用 CloudWatch 控制台、或 CloudWatch API 来检查 Performance Insights 指标。 AWS CLI您也可以像添加任何其他指标一样添加 CloudWatch警

报。例如，如果DBLoad指标违反了您设置的阈值，您可能希望触发向 DBA 的短信通知或采取纠正措施。您还可以将 Performance Insights 指标添加到现有 CloudWatch仪表板中。

增强监控

增强监控是一种实时捕获运行 Amazon RDS 数据库实例的操作系统 (OS) 指标的工具。这些指标为 CPU、内存、Amazon RDS 和操作系统进程、文件系统和磁盘 I/O 数据等提供高达一秒的粒度。您可以在 Amazon RDS 控制台中访问和分析这些指标。与 Performance Insights 一样 CloudWatch，增强型监控指标从 Amazon RDS 传输到，您可以从其他功能中受益，例如长期保存指标以供分析、创建指标筛选器、在 CloudWatch 控制面板上显示图表以及设置警报。默认情况下，当您创建新的 Amazon RDS 数据库实例时，“增强监控” 处于禁用状态。您可以在创建或修改数据库实例时启用该功能。定价基于从 Amazon RDS 传输到 CloudWatch 日志的数据量和存储费率。根据启用增强监控的数据库实例的粒度和数量，部分监控数据可以包含在 CloudWatch 日志免费套餐中。有关完整的定价详情，请参阅 Amazon CloudWatch 定价。有关该工具的更多信息，请参阅 Amazon RDS 文档和增强监控常见问题解答。

其他 AWS 服务

AWS 提供了多种支持服务，这些服务还与 Amazon RDS 集成 CloudWatch，并进一步增强数据库的可观察性。其中包括 Amazon EventBridge、Amaz CloudWatch on Logs 和 AWS CloudTrail。

- Amazon EventBridge 是一个无服务器事件总线，可以接收、筛选、转换、路由和传送来自您的应用程序和 AWS 资源（包括 Amazon RDS 数据库实例）的事件。A mazon RDS 事件表示亚马逊 RDS 环境发生了变化。例如，当数据库实例的状态从 “可用” 更改为 “已停止” 时，Amazon RDS 会生成事件`RDS-EVENT-0087 / The DB instance has been stopped`。Amazon RDS 以近乎实时的方式将 CloudWatch 事件传送到活动 EventBridge 中。使用 EventBridge 和 CloudWatch 事件，您可以定义规则，以便针对感兴趣的特定 Amazon RDS 事件发送警报，并在事件符合规则时自动执行操作。有多种目标可用于响应事件，例如可以执行更正操作的 AWS Lambda 功能，或者可以发送电子邮件或短信通知数据库管理员或 DevOps 工程师有关事件的 Amazon SNS 主题。
- Amazon Lo CloudWatch gs 是一项集中存储所有应用程序、系统和服务的日志文件的 AWS 服务，包括适用于 MySQL 的 Amazon RDS 和 MariaDB 数据库实例以及。 AWS CloudTrail如果您为数据库实例启用该功能，Amazon RDS 会自动将以下日志发布到 CloudWatch 日志：
  - 错误日志
  - 慢速查询日志
  - 常规日志
  - 审计日志

您可以使用 CloudWatch Logs Insights 来查询和分析日志数据。该功能包括一种专门构建的查询语言，可帮助您搜索与您定义的模式相匹配的日志事件。例如，您可以通过监视以下模式的错误日志文件来跟踪 MySQL 数据库实例中的表损坏："ERROR 1034 (HY000): Incorrect key file for table '*'; try to repair it OR Table * is marked as crashed"。筛选后的日志数据可以转换为 CloudWatch 指标。然后，您可以使用这些指标创建包含图表或表格数据的仪表板，或者在超过定义的阈值时设置警报。这在使用审核日志时特别有用，因为如果检测到任何意外或可疑行为，您可以自动监控、发送警报并采取纠正措施。您可以使用 AWS 管理控制台、、Amazon RDS API 或日志 AWS 软件开发工具包来访问和管理数据库 CloudWatch 日志。 AWS CLI

- AWS CloudTrail记录并持续监控您的 AWS 账户中的用户和 API 活动。它可以帮助您对适用于 MySQL 的 Amazon RDS 或 MariaDB 数据库实例进行审计、安全监控和操作故障排除。 CloudTrail 已与 Amazon RDS 集成。可以记录所有操作，并 CloudTrail 记录用户、角色或 AWS 服务在 Amazon RDS 中执行的操作。例如，当用户创建新的 Amazon RDS 数据库实例时，会检测到一个事件，并且日志包含有关请求的操作 ("eventName": "CreateDBInstance")、操作的日期和时间 ("eventTime": "2022-07-30T22:14:06Z")、请求参数 ("requestParameters": {"dBInstanceIdentifier": "test-instance", "engine": "mysql", "dBInstanceClass": "db.m6g.large"}) 等的信息。记录的事件 CloudTrail 包括来自亚马逊 RDS 控制台的调用和来自使用 Amazon RDS API 的代码的调用。

第三方监控工具

在某些情况下，除了为 Amazon RDS AWS 提供的全套云原生可观察性和监控工具外，您可能还需要使用其他软件供应商提供的监控工具。此类场景包括混合部署，在这种部署中，您的本地数据中心可能运行多个数据库，而另一组数据库则在中运行 AWS Cloud。如果您已经建立了企业可观察性解决方案，则可能需要继续使用现有工具并将其扩展到您的 AWS 云部署。设置第三方监控解决方案的挑战通常在于作为云托管服务的 Amazon RDS 所实施的保护措施。例如，您无法在运行数据库实例的主机操作系统上安装代理软件，因为对数据库主机的访问被拒绝。但是，您可以通过在其他 AWS Cloud 服务之上进行构建，将许多第三方监控解决方案与 Amazon RDS 集成。 CloudWatch 例如，可以导出 Amazon RDS 指标、日志、事件和跟踪，然后将其导入第三方监控工具，以进行进一步分析、可视化和警报。其中一些第三方解决方案包括Prometheus、Grafana和Percona。

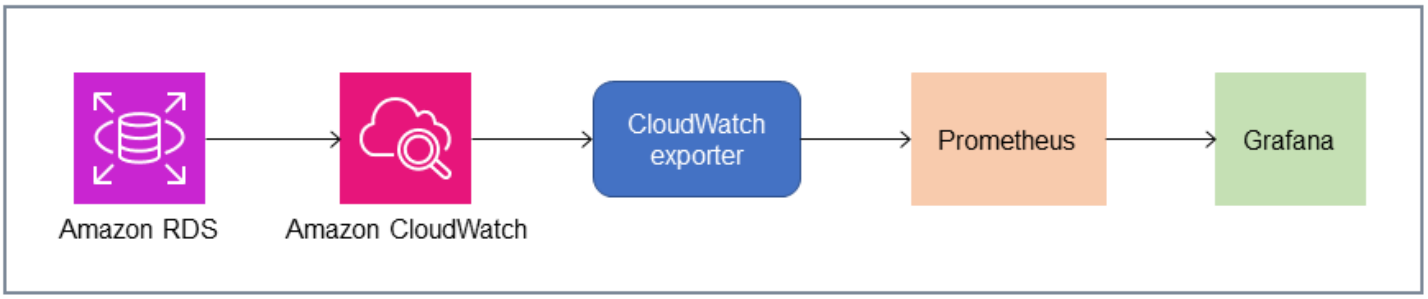
Prometheus 和 Grafana

Prometheus 是一种开源监控解决方案，可按给定的间隔从配置的目标收集指标。它是一种通用监控解决方案，可以监控任何应用程序或服务。当您监控 Amazon RDS 数据库实例时， CloudWatch 会从 Amazon RDS 收集指标。然后，使用开源导出器（例如 YACE 导出器或导出器）将指标导出到 Prometheus 服务器。 CloudWatch

- YACE 导出器通过在 API 的单个请求中检索多个指标来优化数据导出任务。 CloudWatch 指标存储在 Prometheus 服务器上后，服务器会评估规则表达式，并在观察到指定条件时生成警报。
- CloudWatch 出口商由 Prometheus 正式维护。它通过 CloudWatch API 检索 CloudWatch 指标，并使用对 HTTP 端点的 REST API 请求，以与 Prometheus 兼容的格式将其存储在 Prometheus 服务器上。

在选择导出器、设计部署模型和配置导出器实例时，请考虑CloudWatch并CloudWatch 记录服务和 API 配额，因为将 CloudWatch 指标导出到 Prometheus 服务器是在 API 之上实现的。 CloudWatch 例如，在单个 AWS 账户 和区域中部署多个 Exporter 实例来监控数百个 Amazon RDS 数据库实例，可能会导致限制错误 (ThrottlingException) 和代码 400 错误。 CloudWatch 要克服这些限制，可以考虑使用 YACE 导出器，该导出器经过优化，可在单个请求中收集多达 500 个不同的指标。此外，要部署大量 Amazon RDS 数据库实例，您应考虑使用多个实例 AWS 账户，而不是将工作负载集中到单个实例中 AWS 账户，并限制每个 AWS 账户实例中的导出器实例数量。

警报由 Prometheus 服务器生成并由 Alertmanager 处理。该工具负责对警报进行重复数据删除、分组和路由到正确的接收者，例如电子邮件、短信或 Slack，或者启动自动响应操作。另一个名为 Grafana 的开源工具显示这些指标的可视化效果。Grafana 提供了丰富的可视化控件，例如高级图表、动态仪表板以及临时查询和动态深入分析等分析功能。它还可以搜索和分析日志，并包括警报功能，以持续评估指标和日志，并在数据与警报规则匹配时发送通知。



Percona

P@@ ercona监控和管理（PMM）是一款免费的开源数据库监控、管理和可观察性解决方案，适用于MySQL和MariaDB。PMM 从数据库实例及其主机收集数千个性能指标。它提供了用于在仪表板中可视化数据的 Web 用户界面以及其他功能，例如用于数据库运行状况评估的自动顾问。您可以使用 PMM 来监控 Amazon RDS。但是，PMM 客户端（代理）未安装在 Amazon RDS 数据库实例的底层主机上，因为它无法访问这些主机。相反，该工具连接到 Amazon RDS 数据库实例，查询服务器统计信息`INFORMATION_SCHEMA`、系统架构和性能架构，并使用 CloudWatch API 获取指标、日志、事件和跟踪。PMM 需要一个 AWS Identity and Access Management (IAM) 用户访问密钥（IAM 角色），并会自动发现可供监控的 Amazon RDS 数据库实例。与 Prometheus 相比，PMM 工具被配置

为用于数据库监控，它收集的数据库特定指标更多。要使用 PMM 查询分析控制面板，必须将性能架构配置为查询源，因为未为 Amazon RDS 安装查询分析代理，也无法读取慢速查询日志。相反，它直接`performance_schema`从 MySQL 和 MariaDB 数据库实例中查询，以获取指标。PMM的突出特点之一是它能够就该工具在其数据库中发现的问题向数据库管理员发出警报和建议。PMM 提供一系列检查，可以检测常见的安全威胁、性能下降、数据丢失和数据损坏。

除了这些工具之外，市场上还有几种可与 Amazon RDS 集成的商业可观察性和监控解决方案。示例包括 Datadog 数据库监控、Dy natrace Amazon RDS 监控和数据库监控。AppDynamics

数据库实例监控

一个数据库实例是 Amazon RDS 的基本构件。它是在云中运行的隔离数据库环境。对于 MySQL 和 MariaDB 数据库，数据库实例是mysqld程序，也称为 MySQL 服务器，它包括多个线程和组件，例如 SQL 解析器、查询优化器、线程/连接处理器、系统和状态变量以及一个或多个可插拔存储引擎。每个存储引擎都旨在支持特殊用例。默认和推荐的存储引擎是InnoDB，它是一个事务性、通用性、关系数据库引擎，符合原子性、一致性、隔离、耐久性 (ACID) 模型。InnoDB 功能内存中的结构（缓冲池、更改缓冲区、自适应哈希索引、日志缓冲区）以及磁盘上的结构（表空间、表、索引、撤消日志、重做日志、双写缓冲区文件）。为确保您的数据库严格遵守 ACID 模型，InnoDB 存储引擎实现了多种功能保护您的数据，包括事务、提交、回滚、崩溃恢复、行级锁定和多版本并发控制 (MVCC)。

数据库实例的所有这些内部组件协同工作，有助于将数据的可用性、完整性和安全性保持在预期和令人满意的性能水平。根据您的工作负载，每个组件和功能可能会对 CPU、内存、网络和存储子系统施加资源需求。当对特定资源的需求激增超过该资源的预配置容量或软件限制（由配置参数或软件设计施加）时，数据库实例可能会出现性能下降或完全不可用和损坏。因此，必须测量和监控这些内部组件，将它们与定义的基准值进行比较，并在监控值与预期值偏离时生成警报。

如前所述，你可以使用不同的工具监控你的 MySQL 和 MariaDB 实例。我们建议您使用 Amazon RDS 性能见解和CloudWatch用于监控和警报的工具，因为这些工具已与 Amazon RDS 集成，可收集高分辨率指标，近乎实时地显示最新的性能信息，并生成警报。

无论您的首选监控工具是什么，我们都建议您打开性能架构在你的 MySQL 和 MariaDB 数据库实例中。这个性能架构是一项可选功能，用于在低级别监控 MySQL 服务器（数据库实例）的操作，旨在将对数据库整体性能的影响降至最低。您可以使用以下方法管理此功能`performance_schema`参数。尽管此参数是可选的，但您必须使用它来收集每个 SQL 的高分辨率（一秒）指标、活动会话指标、等待事件和其他详细的低级别监控信息，这些信息由 Amazon RDS Performance Insights 收集。

章节

- 数据库实例的性能洞察指标
- CloudWatch数据库实例的指标
- 将绩效洞察指标发布到CloudWatch

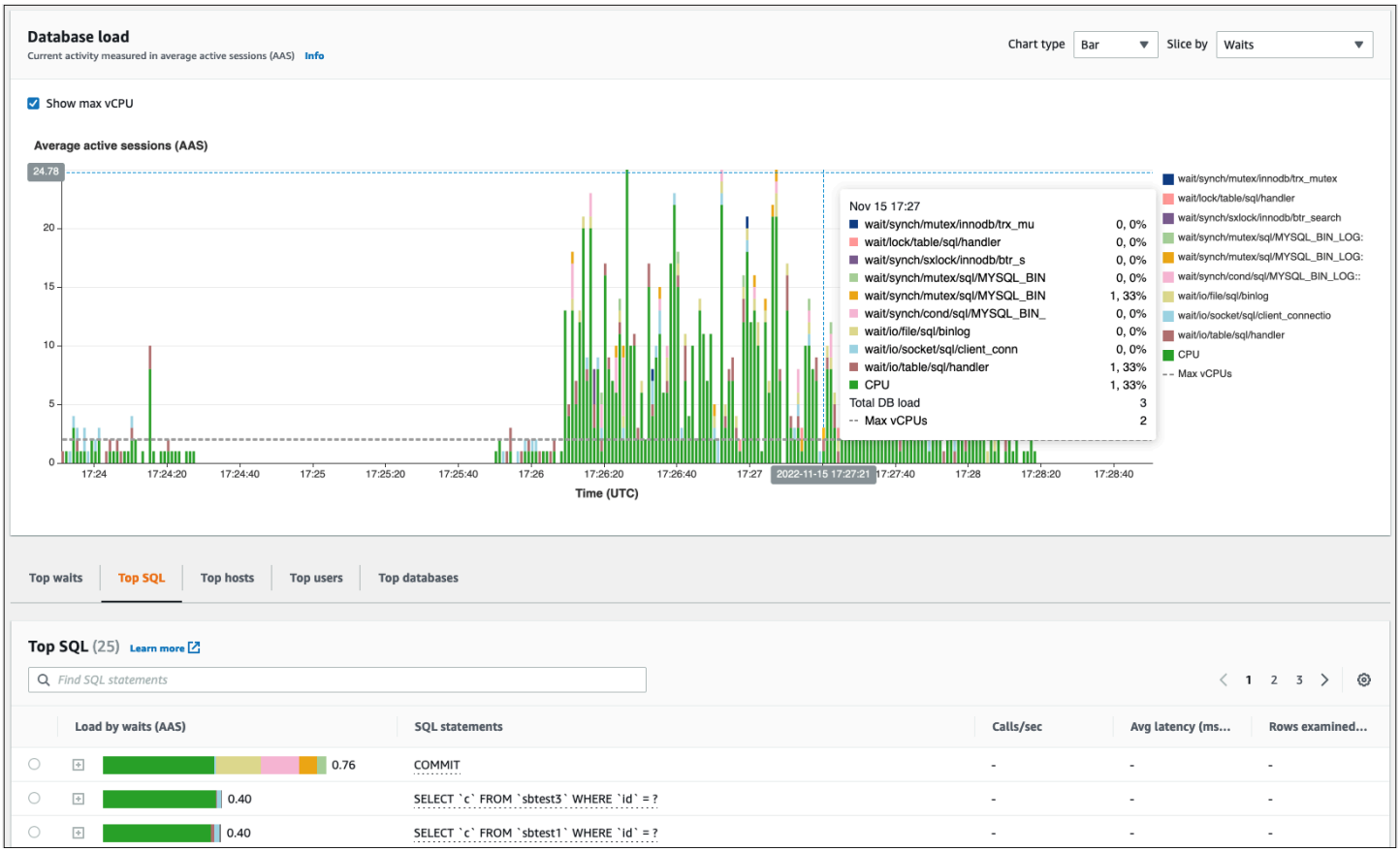
数据库实例的性能洞察指标

性能洞察可监控不同类型的指标，如以下各节所述。

数据库负载

数据库加载 (DBLoad) 是 Performance Insights 中的一项关键指标，用于衡量数据库中的活动水平。每秒收集一次并自动发布到亚马逊CloudWatch。它表示数据库实例在平均活动会话 (AAS) 中的活动，即同时运行 SQL 查询的会话数量。这个DBLoad指标与其他时间序列指标不同，因为可以使用以下五个维度中的任何一个来解释它：等待、SQL、主机、用户和数据库。这些维度是的子类别DBLoad公制。你可以把它们用作切成薄片类别代表数据库负载的不同特征。有关我们如何计算数据库负载的详细描述，请参见数据库加载在亚马逊 RDS 文档中。

以下屏幕插图显示了性能洞察工具。



维度

- 等待活动是数据库会话等待资源或其他操作完成才能继续处理的情况。如果你运行一个 SQL 语句，比如`SELECT * FROM big_table`如果这个表比分配的InnoDB缓冲池大得多，你的会话很可能会等待`wait/io/file/innodb/innodb_data_file`等待事件，由数据文件上的物理 I/O 操作引起。等待事件是数据库监控的重要维度，因为它们表明可能存在性能瓶颈。等待事件表示您在会话中运行的 SQL 语句等待时间最多的资源和操作。例如，`wait/synch/mutex/innodb/trx_sys_mutex`当数据库活动频繁且有大量事务时，就会发生事件，并且`wait/synch/mutex/`

`innodb/buf_pool_mutex`当线程在InnoDB缓冲池上获得锁定以访问内存中的页面时，就会发生事件。有关所有 MySQL 和 MariaDB 等待事件的信息，请参见等待事件摘要表在 MySQL 文档中。要了解如何解释乐器名称，请参见性能架构仪器命名惯例在 MySQL 文档中。

- SQL显示哪些 SQL 语句对数据库总负载的贡献最大。这个顶部尺寸桌子，位于数据库加载Amazon RDS 性能洞察中的图表是交互式的。您可以通过单击 SQL 语句中的栏来获取与 SQL 语句相关的等待事件的详细列表等待加载 (AAS)专栏。当您在列表中选择 SQL 语句时，Performance Insights 会在列表中显示相关的等待事件数据库加载图表和中的 SQL 语句文本SQL 文本部分。SQL 统计信息显示在右侧顶部尺寸桌子。
- 主持人显示连接的客户机的主机名。此维度可帮助您确定哪些客户端主机将大部分负载发送到数据库。
- 用户按登录到数据库的用户对数据库负载进行分组。
- 数据库按客户端连接的数据库的名称对数据库负载进行分组。

计数器指标

计数器指标是累积指标，其值只能在数据库实例重启时增加或重置为零。计数器指标的值不能减少到其先前的值。这些指标代表一个单调递增的计数器。

- 原生计数器是由数据库引擎定义的指标，而不是由 Amazon RDS 定义的指标。例如：
  - `SQL.Innodb_rows_inserted`表示插入到 InnoDB 表中的行数。
  - `SQL.Select_scan`表示完成对第一个表的完整扫描的联接数。
  - `Cache.Innodb_buffer_pool_reads`表示 InnoDB 引擎无法从缓冲池检索而必须直接从磁盘读取的逻辑读取次数。
  - `Cache.Innodb_buffer_pool_read_requests`表示逻辑读取请求的数量。

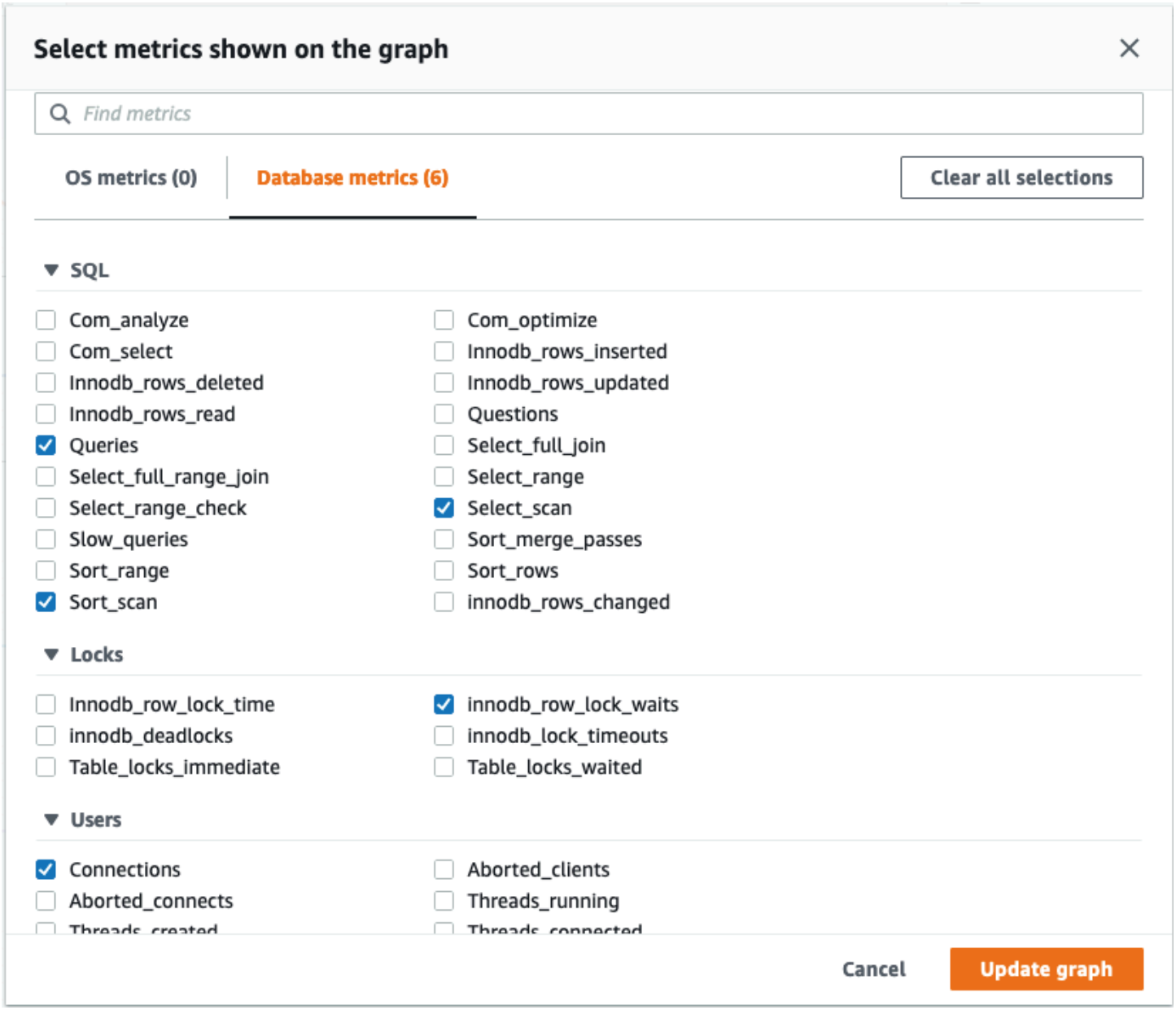
  有关所有原生指标的定义，请参见服务器状态变量在 MySQL 文档中。
- 非原生计数器由亚马逊 RDS 定义。您可以使用特定查询获取这些指标，也可以在计算中使用两个或多个本地指标来获取这些指标。非原生计数器指标可以表示延迟、比率或命中率。例如：
  - `Cache.innoDB_buffer_pool_hits`表示 InnoDB 在不使用磁盘的情况下可以从缓冲池检索的读取操作数。它是根据本地计数器指标计算得出的，如下所示：

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

  - `IO.innoDB_datafile_writes_to_disk`表示 InnoDB 数据文件写入磁盘的操作次数。它仅捕获对数据文件的操作，不捕获双重写入或重做记录写入操作。其计算方法如下：

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

您可以直接在 Performance Insights 控制面板中可视化数据库实例指标。选择管理指标，选择数据库指标选项卡，然后选择感兴趣的指标，如下图所示。



选择更新图表按钮显示您选择的指标，如下图所示。

SQL 统计数据

Performance Insights 收集有关查询运行的每一秒和每个 SQL 调用的 SQL 查询的性能相关指标。一般而言，绩效洞察会收集SQL 统计信息在陈述和摘要层面。但是，对于 MariaDB 和 MySQL 数据库实例，统计数据仅在摘要级别收集。

- 摘要统计数据是所有具有相同模式但最终具有不同文字值的查询的复合指标。摘要用变量替换特定的文字值；例如：

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

- 有些指标代表统计数据每秒适用于每条摘要的 SQL 语句。例如，`sql_tokenized.stats.count_star_per_sec`表示每秒的调用次数（即每秒 SQL 语句运行了多少次）。
- 绩效洞察还包括以下指标：每次通话SQL 语句的统计信息。例如，`sql_tokenized.stats.sum_timer_wait_per_call`显示每次调用 SQL 语句的平均延迟，以毫秒为单位。

SQL 统计信息可在 “性能见解” 仪表板中找到热门的 SQL的选项卡顶部尺寸桌子。

CloudWatch数据库实例的指标

亚马逊CloudWatch还包含 Amazon RDS 自动发布的指标。中的指标AWS/RDS命名空间是实例级指标，指的是 Amazon RDS（服务）实例（即在云中运行的隔离数据库环境），而不是严格意义上的数据库实例mysqld进程。因此，其中大多数默认指标根据该术语的严格定义，属于操作系统指标类别。示例包括：CPUUtilization，WriteIOPS，SwapUsage，还有其他人。但是，有一些数据库实例指标适用于 MariaDB 和 MySQL：

- BinLogDiskUsage— 二进制日志占用的磁盘空间量。
- DatabaseConnections— 与数据库实例的客户端网络连接数。
- ReplicaLag— 只读副本数据库实例滞后于源数据库实例的时间。

将绩效洞察指标发布到CloudWatch

Amazon RDS 性能见解可监控大多数数据库实例的指标和维度，并通过中的性能见解控制面板提供这些指标和维度AWS管理控制台。此仪表板非常适合数据库故障排除和根本原因分析。但是，无法在 Performance Insights 中为与性能相关的指标创建警报。要根据绩效洞察指标创建警报，你必须将这些指标移至CloudWatch。把指标放进去CloudWatch还允许您访问高级监控功能，例如CloudWatch异常检测，指标数学，以及统计数据，你可以将指标导出到外部监控工具，例如 Prometheus 和 Grafana。

绩效洞察指标不会自动发布到CloudWatch（除了dbLoad 指标）。将数据库实例指标从 Performance Insights 发布到CloudWatch，你可以使用性能洞察 API检索指标，以及CloudWatchAPI将指标发布到CloudWatch。要实现流程自动化，您可以创建 Lambda 函数并在亚马逊中对其进行调度EventBridge在指定的时间段运行——例如，每两分钟运行一次。您可以指定要发布到哪些绩效见解指标CloudWatch。Lambda 函数从所有启用了性能洞察的 Amazon RDS 实例获取这些指标，并将这些指标保存在CloudWatch。有关此过程的更多信息，请参阅有关的博客文章将绩效洞察计数器指标提供给CloudWatch。

操作系统监控

适用于 MySQL 的 Amazon RDS 或 MariaDB 中的数据库实例在 Linux 操作系统上运行，该操作系统使用底层系统资源：CPU、内存、网络和存储。

```
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)
```

数据库和底层操作系统的整体性能在很大程度上取决于系统资源的利用率。例如，CPU 是系统性能的关键组件，因为它运行数据库软件指令并管理其他系统资源。如果 CPU 过度使用（即，如果负载所需的 CPU 功率超过为数据库实例配置的功率），则此问题将影响数据库的性能和稳定性，进而影响应用程序的性能和稳定性。

数据库引擎动态分配和释放内存。当 RAM 中没有足够的内存来完成当前工作时，系统会将内存页写入磁盘上的交换内存。由于磁盘比内存慢得多，即使磁盘基于 SSD NVMe 技术，过多的内存分配也会导致性能下降。高内存利用率会增加数据库响应的延迟，因为页面文件的大小会增加以支持额外的内存。如果内存分配过高以致耗尽 RAM 和交换内存空间，则数据库服务可能变得不可用，用户可能会发现错误，例如`[ERROR] mysqld: Out of memory (Needed xyz bytes)`。

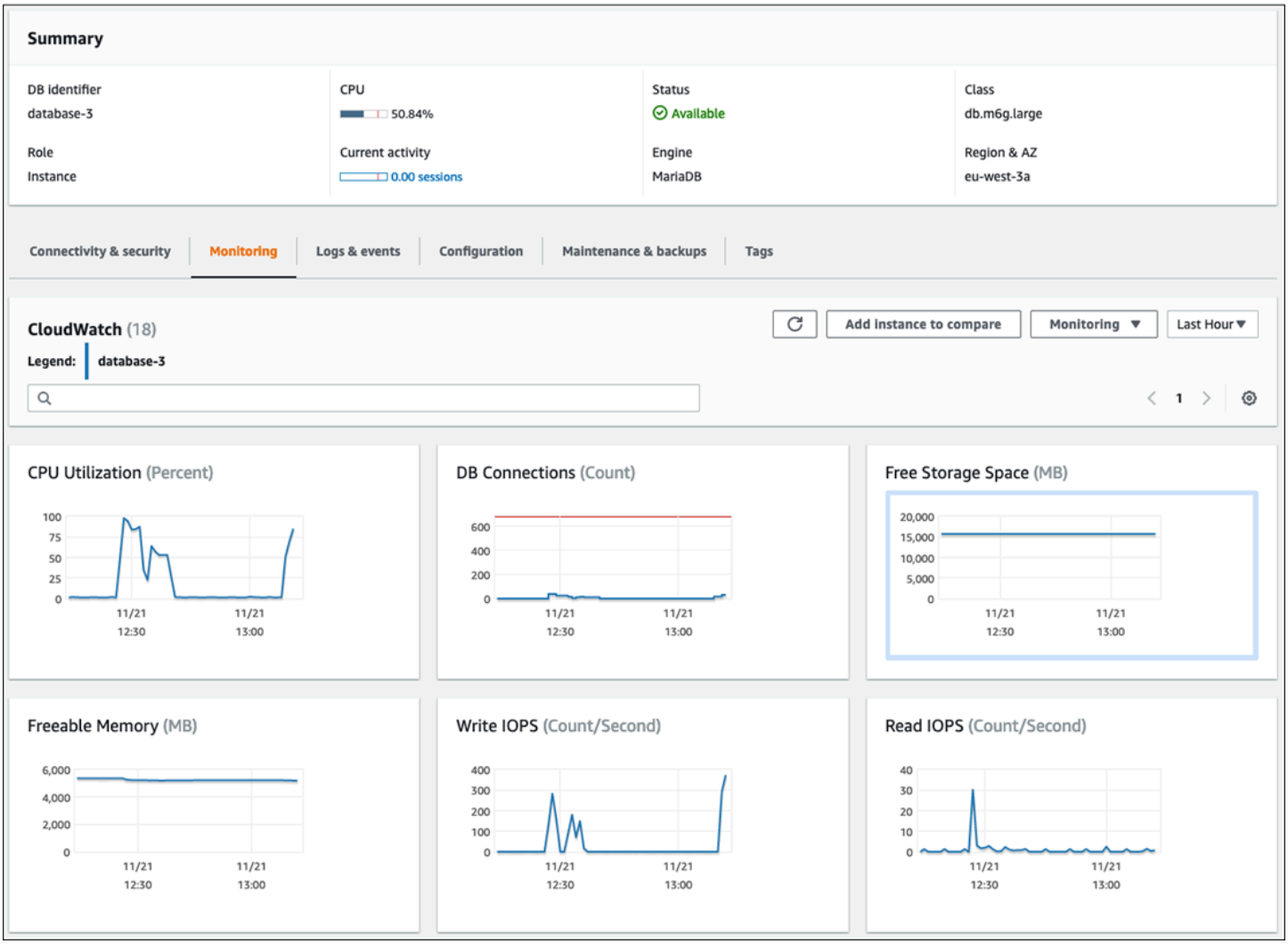
MySQL 和 MariaDB 数据库管理系统使用存储子系统，该子系统由用于存储的磁盘组成磁盘上的结构例如表、索引、二进制日志、重做日志、撤消日志和双重写缓冲区文件。因此，与其他类型的软件相比，数据库必须执行大量的磁盘活动。为了使数据库实现最佳运行，必须监控和调整磁盘 I/O 利用率和磁盘空间分配。当数据库达到磁盘支持的最大 IOPS 或吞吐量的限制时，数据库性能可能会受到影响。例如，索引扫描引起的随机访问突发可能会导致每秒大量的 I/O 操作，最终可能会达到底层存储的限制。全表扫描可能未达到 IOPS 限制，但可能会导致以兆字节每秒为单位的高吞吐量。监控和生成有关磁盘空间分配的警报至关重要，因为错误，例如`OS error code 28: No space left on device`可能会导致数据库不可用和损坏。

Amazon RDS 为运行数据库实例的操作系统实时提供指标。Amazon RDS 会自动将一组操作系统指标发布到CloudWatch。这些指标可供您在 Amazon RDS 控制台和CloudWatch仪表板，您可以在中对所选指标设置警报CloudWatch。示例包括：

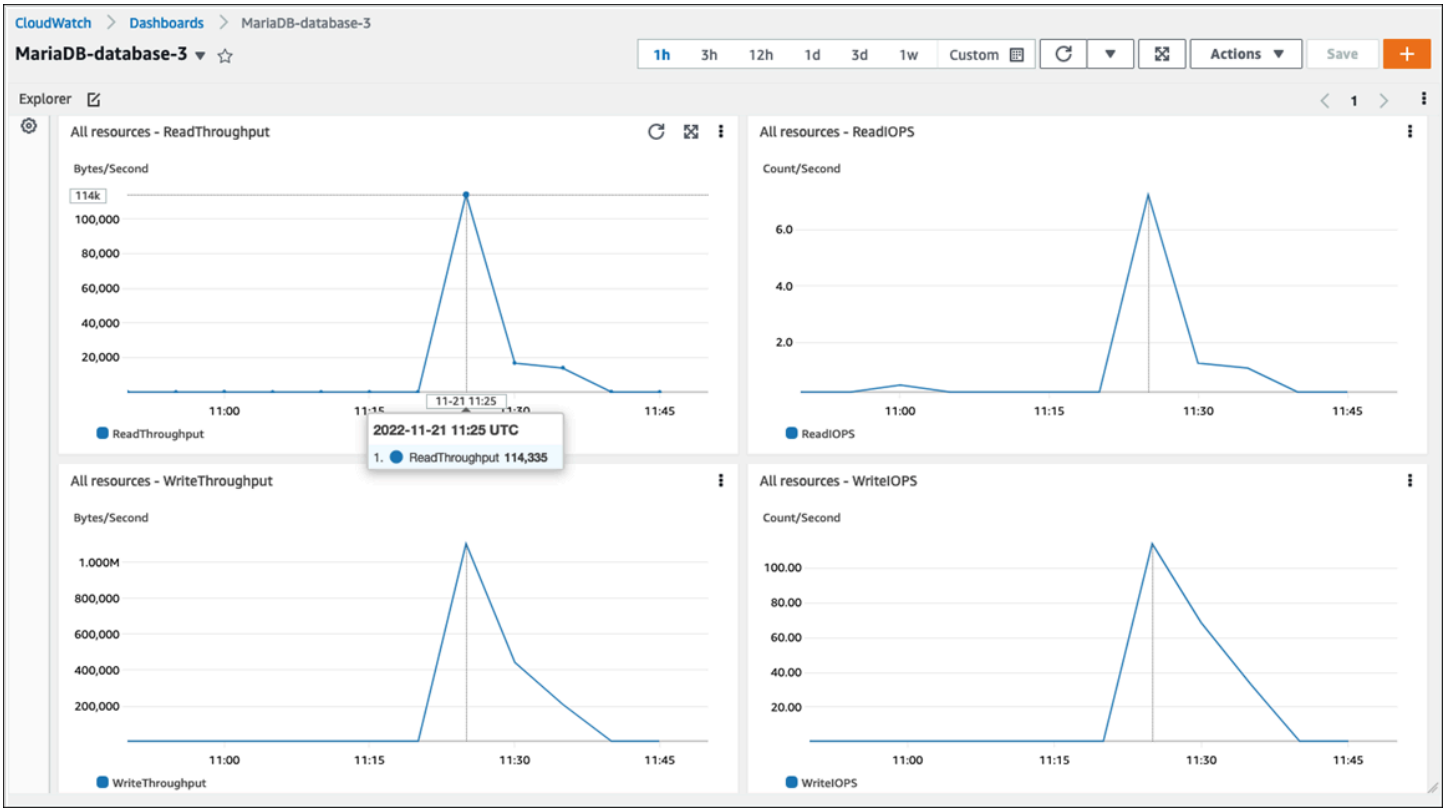
- `CPUUtilization`— CPU 利用率的百分比。
- `BinLogDiskUsage`— 二进制日志占用的磁盘空间量。
- `FreeableMemory`— 可用的随机存取内存量。这代表了的价值`MemAvailable`的字段`/proc/meminfo`。
- `ReadIOPS`— 每秒磁盘读取 I/O 操作的平均次数。
- `WriteThroughput`— 本地存储每秒写入磁盘的平均字节数。
- `NetworkTransmitThroughput`— 数据库节点上的传出网络流量，它结合了数据库流量和用于监控和复制的 Amazon RDS 流量。

有关 Amazon RDS 发布的所有指标的完整参考信息CloudWatch，参见亚马逊CloudWatch亚马逊 RDS 的指标在亚马逊 RDS 文档中。

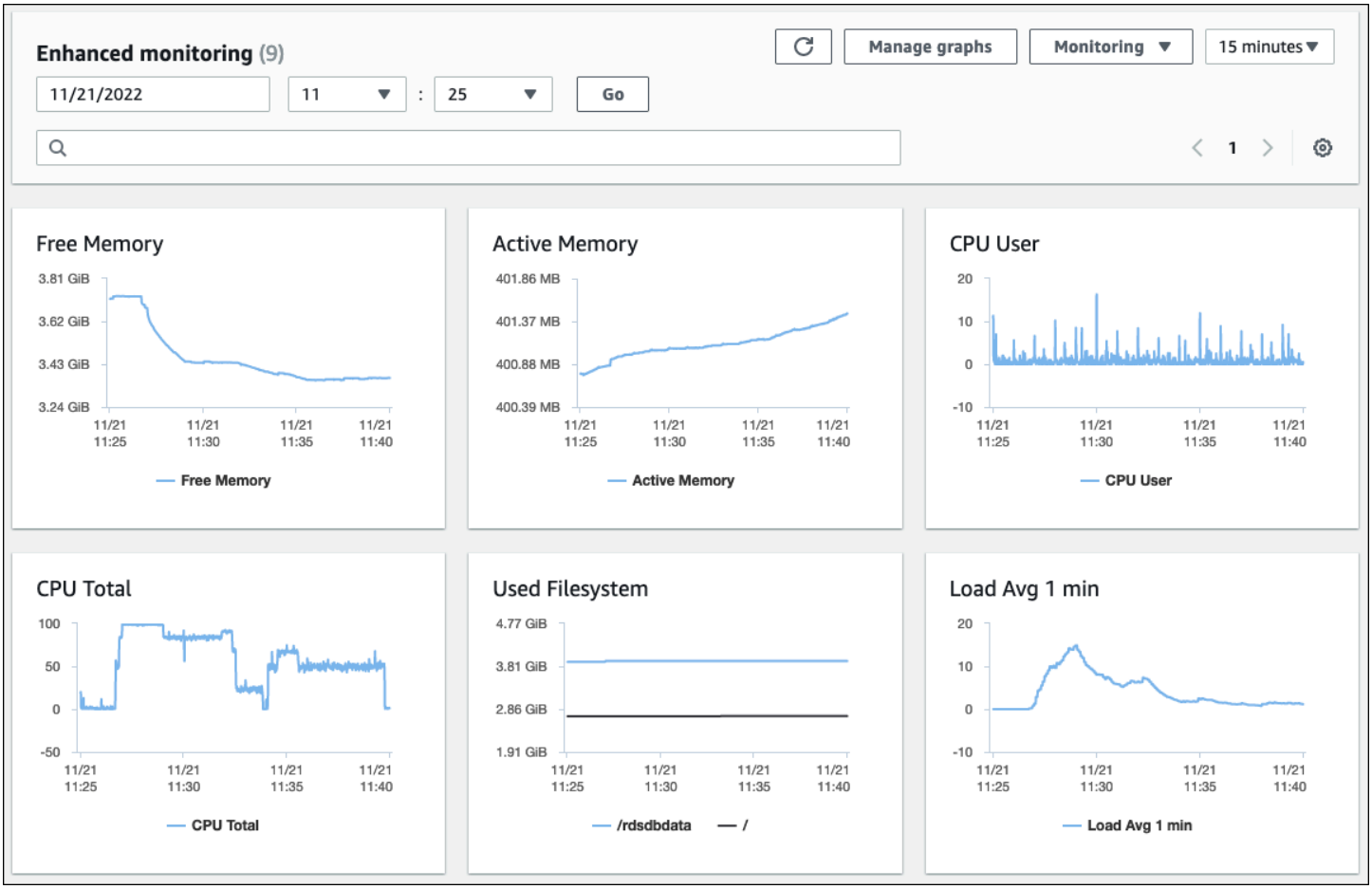
下图显示了以下示例CloudWatch亚马逊 RDS 控制台上显示的亚马逊 RDS 指标。



下图显示了显示在中的类似指标CloudWatch仪表板。



另一组操作系统指标由收集增强监控适用于亚马逊 RDS。此工具通过提供实时系统指标和操作系统流程信息，使您可以更深入地了解适用于 MariaDB 的 Amazon RDS 和 Amazon RDS for MySQL 数据库实例的运行状况。当你启用增强监控在您的数据库实例上并设置所需的粒度，该工具会收集操作系统指标和流程信息，您可以在上显示和分析这些指标和流程信息亚马逊 RDS 控制台，如以下屏幕所示。



增强监控提供的一些关键指标是：

- `cpuUtilization.total`— 正在使用的 CPU 的总百分比。
- `cpuUtilization.user`— 用户程序使用的 CPU 百分比。
- `memory.active`— 分配的内存量，以千字节为单位。
- `memory.cached`— 用于缓存基于文件系统的 I/O 的内存量。
- `loadAverageMinute.one`— 最后一分钟请求 CPU 时间的进程数。

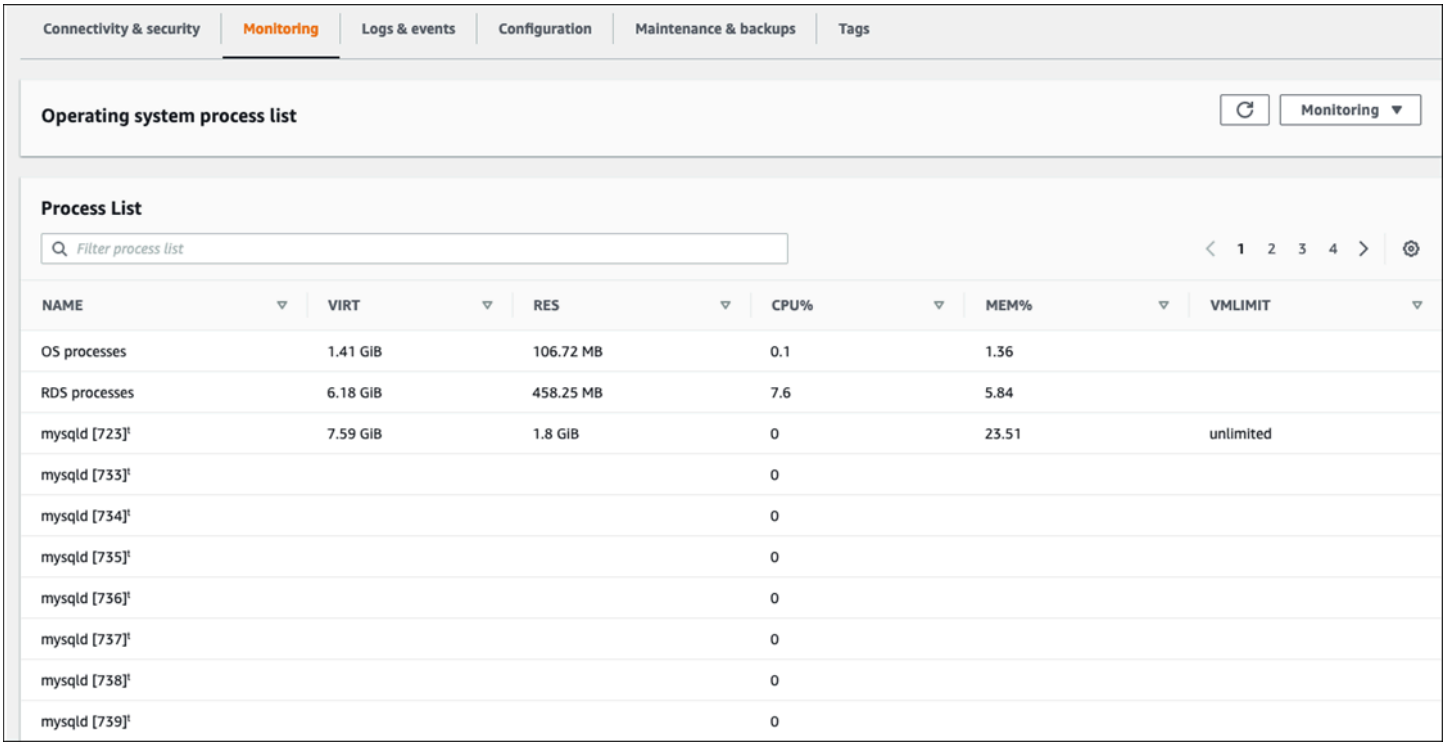
有关指标的完整列表，请参阅增强监控中的操作系统指标在亚马逊 RDS 文档中。

在 Amazon RDS 控制台上，操作系统进程列表提供了数据库实例中正在运行的每个进程的详细信息。该列表分为三个部分：

- 操作系统进程-本部分汇总了所有内核和系统进程。这些过程通常对数据库性能的影响微乎其微。
- RDS 进程— 本节概述了AWS支持 Amazon RDS 数据库实例所需的进程。例如，它包括 Amazon RDS 管理代理、监控和诊断流程以及类似流程。

- RDS 子进程— 本节概述了支持数据库实例的 Amazon RDS 流程，在本例中为`mysqld`进程及其线程。这个`mysqld`话题嵌套在父级下方`mysqld`进程。

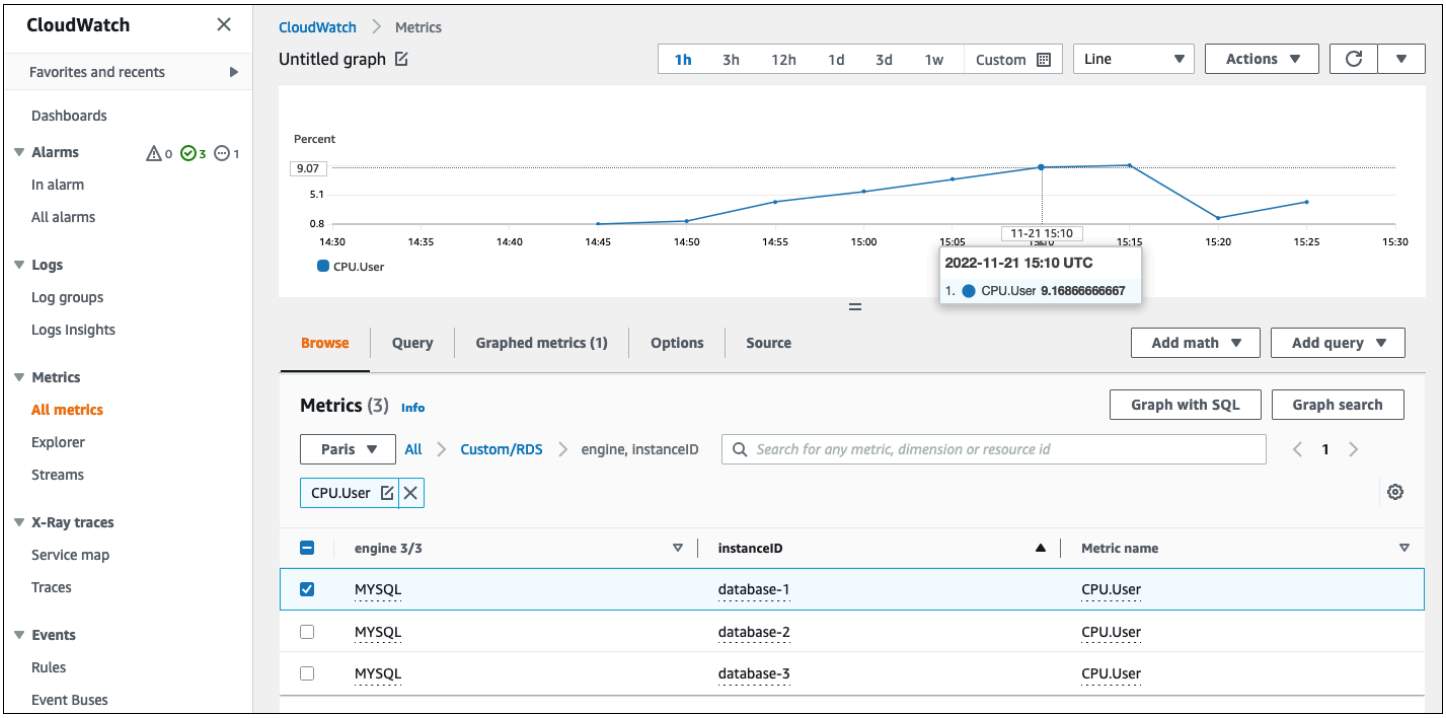
以下屏幕插图显示了 Amazon RDS 控制台中的操作系统进程列表。



Amazon RDS 将增强监控中的指标传送到您的CloudWatch日志账户。在 Amazon RDS 控制台上显示的监控数据是从中检索的CloudWatch日志。你也可以以日志流形式检索数据库实例的指标从CloudWatch日志。这些指标以 JSON 格式存储。您可以使用来自的增强监控 JSON 输出CloudWatch登录您选择的监控系统。

为了在上面显示图表CloudWatch控制面板并创建警报，在指标超过定义的阈值时启动操作，您必须在中创建指标筛选器CloudWatch从CloudWatch日志。有关详细说明，请参见AWS re: Post 文章关于如何筛选增强监控CloudWatch用于为 Amazon RDS 生成自动自定义指标的日志。

以下示例说明了自定义指标`CPU.User`在里面`Custom/RDS`命名空间。此自定义指标是通过筛选创建的`cpuUtilization.user`增强监控指标来自CloudWatch日志。



当指标可用时CloudWatch存储库，你可以在里面显示和分析它CloudWatch仪表板，应用进一步的数学和查询操作，设置警报以监控该特定指标，并在观测值与定义的警报条件不一致时生成警报。

事件、日志和审计追踪

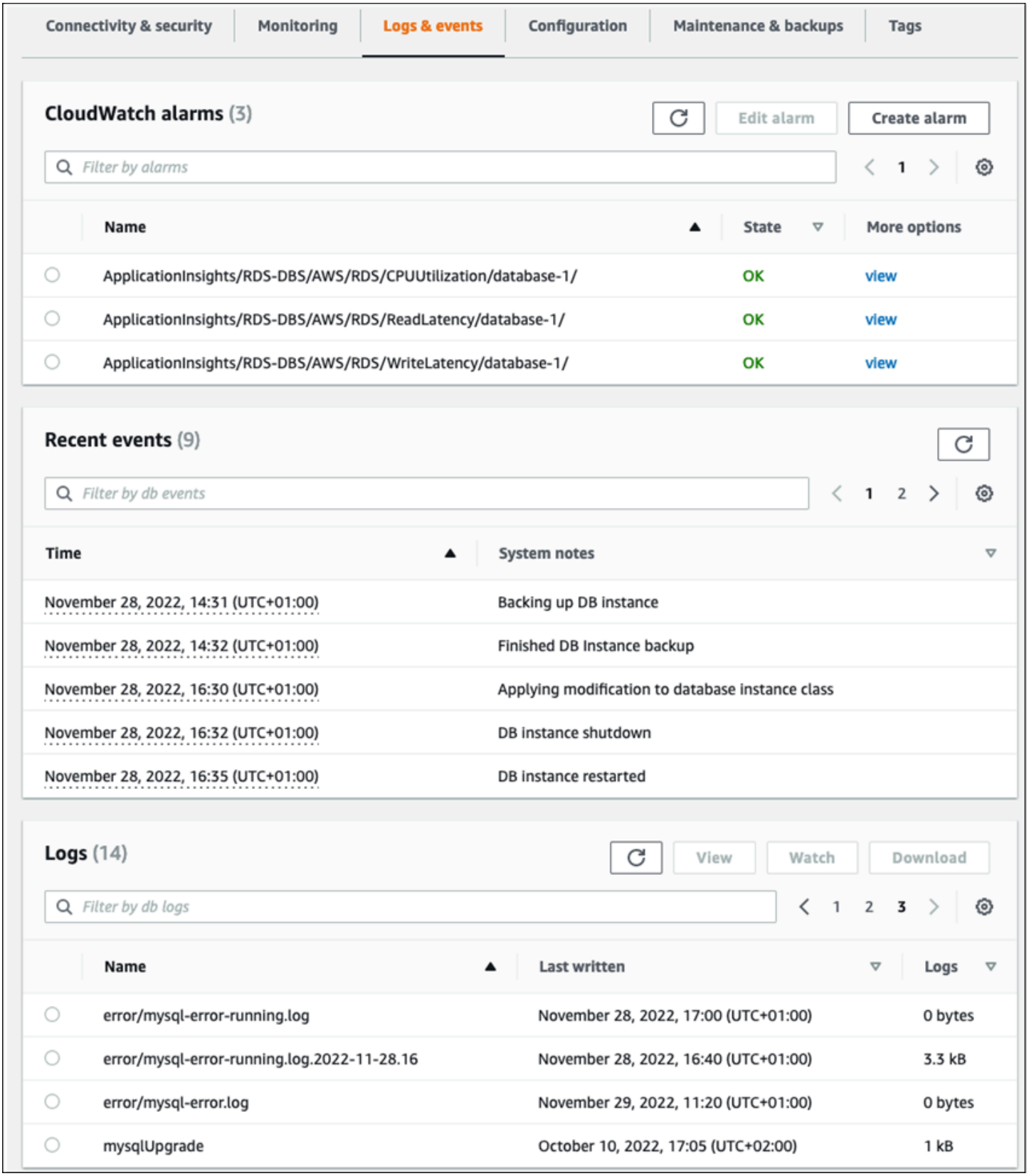
监控数据库实例指标和操作系统指标，分析趋势并将指标与基准值进行比较，以及在值超过定义的阈值时生成警报，这些都是必要的最佳实践，可帮助您实现和维护 Amazon RDS 数据库实例的可靠性、可用性、性能和安全性。但是，完整的解决方案还必须监控 MySQL 和 MariaDB 数据库的数据库事件、日志文件和审计记录。

章节

- 亚马逊 RDS 活动
- 数据库日志
- 审计线索

亚马逊 RDS 活动

一个亚马逊 RDS 活动表示 Amazon RDS 环境发生了变化。例如，当数据库实例状态从正在启动到可用，亚马逊 RDS 会生成事件`RDS-EVENT-0088 The DB instance has been started`。亚马逊 RDS 向亚马逊提供活动EventBridge近乎实时。您可以通过 Amazon RDS 控制台访问事件，AWS CLI 命令描述事件，或者亚马逊 RDS API 操作DescribeEvents。以下屏幕插图显示了 Amazon RDS 控制台上显示的事件和日志。


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 会发出不同类型的事件，包括数据库实例事件、数据库参数组事件、数据库安全组事件、数据库快照事件、RDS 代理事件和蓝/绿部署事件。这些信息包括：

- 源名称和源类型；例如："SourceIdentifier": "database-1", "SourceType": "db-instance"
- 事件的日期和时间；例如："Date": "2022-12-01T09:20:28.595000+00:00"
- 与事件相关的消息；例如："Message": "Finished updating DB parameter group"
- 事件类别；例如："EventCategories": ["configuration change"]

如需完整的参考资料，请参见亚马逊 RDS 事件类别和事件消息在亚马逊 RDS 文档中。

我们建议您监控 Amazon RDS 事件，因为这些事件表示数据库实例可用性的状态变化、配置更改、只读副本状态更改、备份和恢复事件、故障事件、对安全组的修改以及许多其他通知。例如，如果您设置了只读副本数据库实例以增强数据库的性能和耐久性，我们建议您监控 Amazon RDS 事件只读副本与数据库实例关联的事件类别。这是因为诸如此类的事件RDS-EVENT-0057 Replication on the read replica was terminated表示您的只读副本不再与主数据库实例同步。向负责团队通知此类事件已发生可能有助于及时缓解问题。亚马逊EventBridge以及其他 AWS 服务，例如AWS Lambda、亚马逊简单队列服务 (Amazon SQS) 和亚马逊简单通知服务 (Amazon SNS) 可以帮助您自动响应系统事件，例如数据库可用性问题或资源更改。

在 Amazon RDS 控制台上，您可以检索过去 24 小时的事件。如果你使用AWS CLI或者使用 Amazon RDS API 查看事件，您可以使用以下方法检索过去 14 天的事件描述事件命令如下。

```
$ 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"
        }
    ]
}
```

如果您想长期存储事件，无论是在指定的到期期之前还是永久存储，都可以使用CloudWatch日志记录有关 Amazon RDS 生成的事件的信息。要实现此解决方案，您可以使用 Amazon SNS 主题接收 Amazon RDS 事件通知，然后调用 Lambda 函数来记录该事件CloudWatch日志。

1. 创建将在事件上调用的 Lambda 函数，并将事件中的信息记录到CloudWatch日志。CloudWatch日志与 Lambda 集成，提供了一种记录事件信息的便捷方式，方法是打印函数变为`stdout`。
2. 通过订阅 Lambda 函数创建 SNS 主题（设置协议到 Lambda），然后设置端点到您在上一步中创建的 Lambda 函数的亚马逊资源名称 (ARN)。
3. 配置您的 SNS 主题以接收 Amazon RDS 事件通知。有关详细说明，请参见AWS回复：发布文章介绍如何让您的亚马逊 SNS 主题接收 Amazon RDS 通知。
4. 在 Amazon RDS 控制台上，创建新的事件订阅。设置目标到 ARN，然后选择您之前创建的 SNS 主题。设置来源类型和要包括的事件类别根据你的要求。有关更多信息，请参见订阅亚马逊 RDS 事件通知在亚马逊 RDS 文档中。

数据库日志

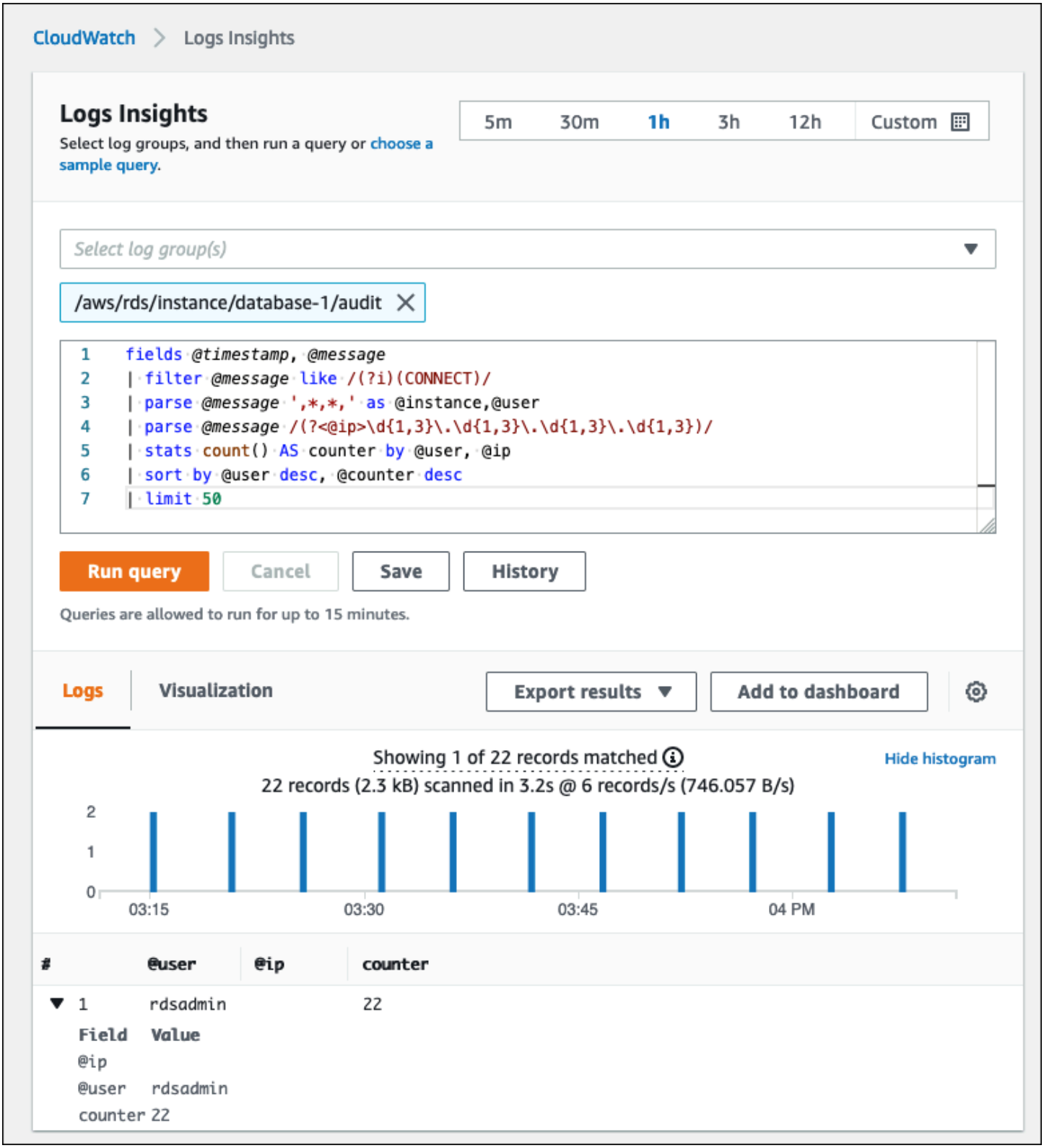
MySQL 和 MariaDB 数据库生成日志，您可以访问这些日志进行审计和故障排除。这些日志是：

- 审计— 审计线索是一组记录服务器活动的记录。对于每个客户端会话，它会记录谁连接到服务器（用户名和主机）、运行了哪些查询、访问了哪些表以及更改了哪些服务器变量。
- 错误— 此日志包含服务器的 (`mysqld`) 启动和关闭时间，以及诊断消息，例如服务器启动和关闭期间以及服务器运行期间出现的错误、警告和注释。
- 普通的— 此日志记录了以下活动`mysqld`，包括每台客户机的连接和断开连接活动，以及从客户端收到的 SQL 查询。当你怀疑有错误并想确切知道客户端发送了什么时，常规查询日志可能非常有用`mysqld`。
- 查询速度慢— 此日志记录了花了很长时间才执行的 SQL 查询。

作为最佳实践，你应该将数据库日志从亚马逊 RDS 发布到亚马逊CloudWatch日志。和CloudWatch日志，您可以对日志数据进行实时分析，将数据存储在高度耐用的存储器中，并使用日志管理数据CloudWatch日志代理。你可以访问和监视您的数据库日志来自亚马逊 RDS 控制台。你也可以使用CloudWatchLogs Insights 可交互式搜索和分析您的日志数据CloudWatch日志。以下示例说明了对审计日志的查询，该查询检查了多少次CONNECT事件出现在日志中，连接了谁以及从哪个客户端（IP 地址）连接。审核日志的摘录可能如下所示：

```
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
```

Log Insights 查询示例显示rdsadmin从以下地址连接到数据库localhost每 5 分钟一次，共计 22 次，如下图所示。这些结果表明，该活动源自内部 Amazon RDS 进程，例如监控系统本身。



日志事件通常包含您想要计算的重要消息，例如与 MySQL 和 MariaDB 数据库实例相关的操作的警告或错误。例如，如果操作失败，则可能会出现错误并按如下方式记录到错误日志文件中：ERROR

1114 (HY000): The table zip_codes is full。您可能需要监控这些条目以了解错误的趋势。你可以创建自定义CloudWatch使用筛选器来自 Amazon RDS 日志的指标启用对 Amazon RDS 数据库日志的自动监控，以监控特定日志中的特定模式，并在出现违反预期行为时生成警报。例如，为日志组创建指标筛选器/aws/rds/instance/database-1/error这将监视错误日志并搜索特定模式，比如ERROR。设置过滤器图案到ERROR和指标值到1。过滤器将检测包含关键字的每条日志记录ERROR，它会将每个包含 “ERROR” 的日志事件的计数增加 1。创建过滤器后，您可以设置警报，以便在 MySQL 或 MariaDB 错误日志中检测到错误时通知您。

要了解有关通过创建监控慢速查询日志和错误日志的更多信息CloudWatch仪表板和使用 CloudWatchLogs Insights，请参阅博客文章创建亚马逊CloudWatch监控亚马逊 RDS 和亚马逊 Aurora MySQL 的仪表

审核跟踪

审计跟踪（或审计日志）提供与安全相关的按时间顺序记录您的 AWS 账户中的事件。它包括 Amazon RDS 的事件，这些事件为影响您的数据库或云环境的活动顺序提供书面证据。在适用于 MySQL 或 MariaDB 的亚马逊 RDS 中，使用审计记录涉及：

- 监控数据库实例审计日志
- 监控中的亚马逊 RDS API 调用AWS CloudTrail

对于 Amazon RDS 数据库实例，审计目标通常包括：

- 为以下各项启用问责制：
  - 对参数或安全配置执行的修改
  - 在数据库架构、表或行中执行的操作，或影响特定内容的操作
- 入侵检测和调查
- 可疑活动检测和调查
- 检测授权问题；例如，识别普通用户或特权用户滥用访问权限的情况

数据库审计线索试图回答以下典型问题：谁查看或修改了数据库中的敏感数据？ 这是什么时候发生的？ 特定用户从哪里访问数据？ 特权用户是否滥用了他们的无限访问权限？

MySQL 和 MariaDB 都使用 MariaDB 审计插件实现了数据库实例审计跟踪功能。此插件记录数据库活动，例如用户登录数据库和针对数据库运行的查询。数据库活动记录存储在日志文件中。若要访问审计日志，数据库实例必须使用具有 MARIADB_AUDIT_PLUGIN 选项的自定义选项组。有关更多信息，请

参见MariaDB 审计插件支持 MySQL在亚马逊 RDS 文档中。审核日志中的记录以插件定义的特定格式存储。您可以在以下位置找到有关审核日志格式的更多详细信息MariaDB 服务器文档。

这个AWS Cloud为你提供审计记录AWS账户由提供AWS CloudTrail服务。CloudTrail将亚马逊 RDS 的 API 调用捕获为事件。所有亚马逊 RDS 操作都会被记录下来。CloudTrail提供用户、角色或其他人在 Amazon RDS 中执行的操作的记录AWS服务。事件包括在... 中采取的行动AWS管理控制台，AWS CLI，以及AWS软件开发工具包和 API。

示例

在典型的审计场景中，您可能需要合并AWS CloudTrail使用数据库审计日志和 Amazon RDS 事件监控进行跟踪。例如，您可能遇到的场景是 Amazon RDS 数据库实例的数据库参数（例如，`database-1`）已修改，您的任务是确定谁进行了修改、更改了什么以及更改何时发生。

要完成任务，请执行以下步骤：

1. 列出发生在数据库实例上的 Amazon RDS 事件`database-1`并确定该类别中是否存在事件`configuration change`那有消息`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. 确定数据库实例正在使用哪个数据库参数组：

```
$ 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. 使用AWS CLI去搜寻CloudTrail事件在那里的区域database-1是在步骤 1 中发现的 Amazon RDS 事件前后的时段内部署的，在哪里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"
}
```


这个CloudTrail事件表明User1带角色Role1从AWS账户 111122223333 修改了数据库参数组mariadb10-6-test，它曾被数据库实例使用database-1上2022-12-01 at 09:18:19 h。修改了两个参数并将其设置为以下值：

- innodb_log_buffer_size = 8388612
- innodb_write_io_threads = 8

额外CloudTrail和CloudWatch日志功能

您可以通过以下方式对过去 90 天内的操作和安全事件进行故障排除事件历史在CloudTrail控制台。要延长保留期并利用其他查询功能，您可以使用AWS CloudTrail湖。和AWS CloudTrailLake，您可以在事件数据存储中保存事件数据长达七年。此外，该服务支持复杂的 SQL 查询，与中简单的键值查找所提供的视图相比，该查询提供了更深入、更可定制的事件视图事件历史。

要监控您的审计记录、设置警报并在发生特定活动时收到通知，您需要配置CloudTrail将其跟踪记录发送到CloudWatch日志。在跟踪记录存储为CloudWatch日志，您可以定义指标筛选器来评估日志事件以

匹配术语、短语或值，并将指标分配给指标筛选器。此外，你可以创建CloudWatch根据您指定的阈值和时间段生成的警报。例如，您可以配置向负责团队发送通知的警报，以便他们可以采取适当的措施。您也可以将 CloudWatch 配置为自动执行操作以响应警报。

提示

在涉及 IT 基础架构和 IT 服务的安全性、可用性、性能和可靠性时，警报是最重要的信息来源之一。它们会通知并告知您的 IT 团队持续存在的安全威胁、中断、性能问题或系统故障。

信息技术基础架构库 (ITIL)，特别是 IT 服务管理 (ITSM) 实践，将自动警报设置为监控和事件管理和事件管理最佳实践的焦点。

事件警报是指监控工具生成警报，将IT环境中的变化、高风险操作或故障通知您的团队和自动化工具（对于可自动执行的项目）。IT 警报是抵御可能演变为重大事件的系统中断或变更的第一道防线。通过自动监控系统并生成中断和风险变更警报，IT 团队可以最大限度地减少停机时间并降低随之而来的高昂成本。

作为最佳实践，AWS架构完善的框架规定你使用监控生成基于警报的通知，以及主动监控和报警。使用CloudWatch或第三方监控服务来设置警报，指示指标何时超出预期界限。

警报管理的目的是建立高效、标准化的程序，通过记录、分类、行动定义和实施、关闭和事后审查活动来处理 IT 相关事件和事件。

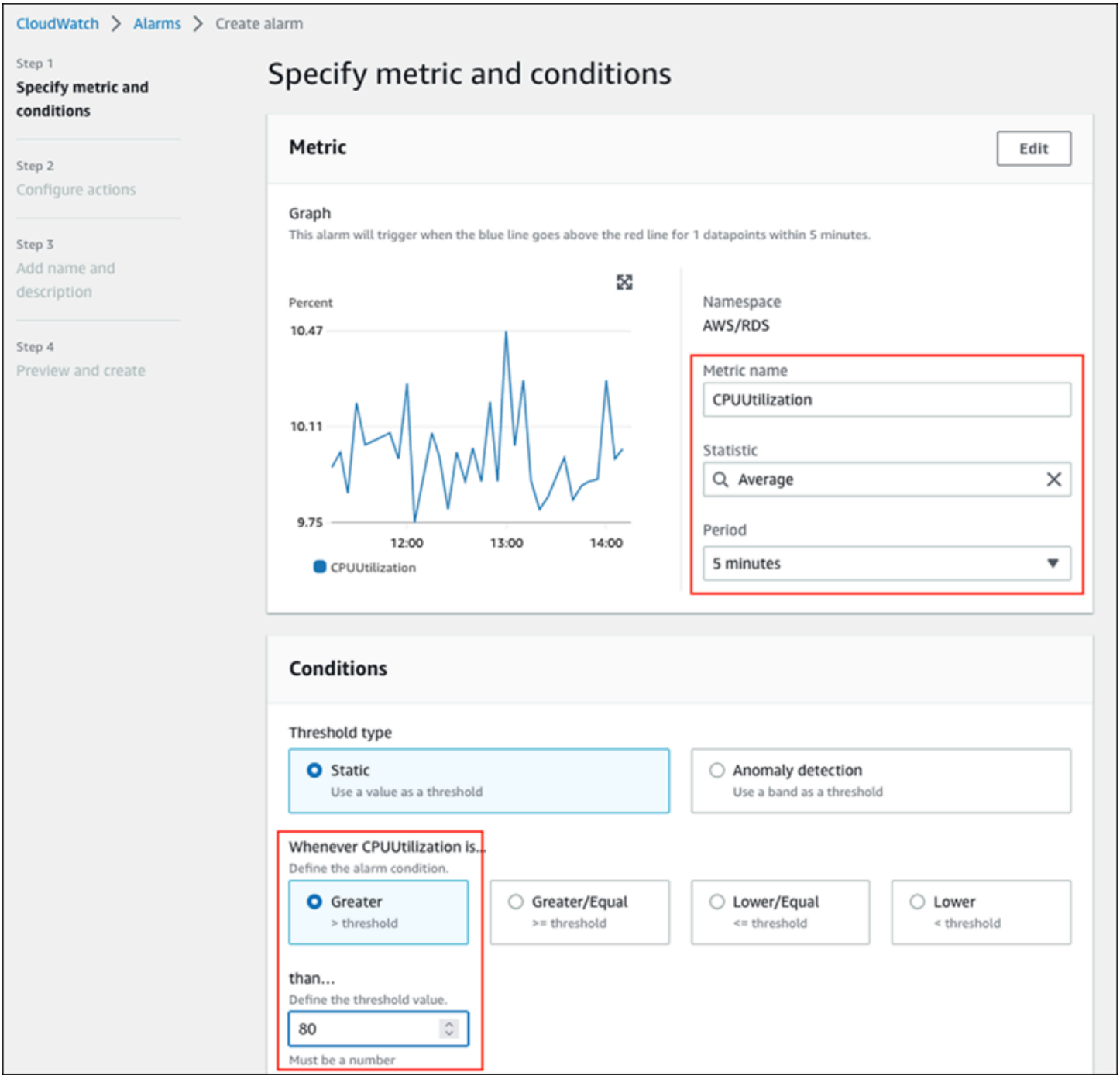
章节

- CloudWatch 警报
- EventBridge规则
- 指定操作、启用和禁用警报

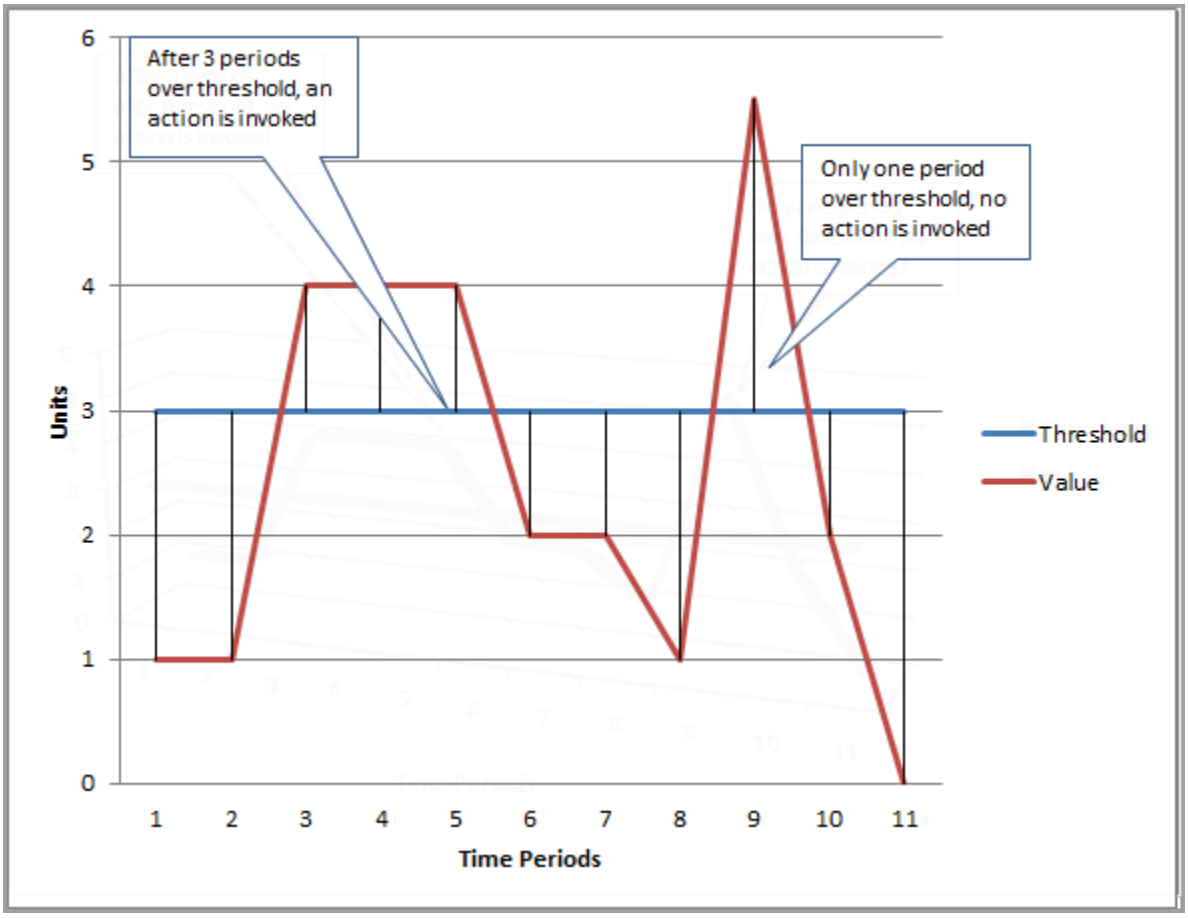
CloudWatch 警报

当您运行 Amazon RDS 数据库实例时，您需要监控不同类型的指标、事件和跟踪并生成警报。对于 MySQL 和 MariaDB 数据库，关键信息来源是数据库实例指标，操作系统指标，事件、日志和审计追踪。我们建议你使用CloudWatch警报在您指定的时间段内观察单个指标。

以下示例说明了如何设置监视警报的警报`CPUUtilization`您的所有 Amazon RDS 数据库实例的指标（CPU 利用率百分比）。您可以将警报配置为在 5 分钟的评估期内任何数据库实例上的 CPU 利用率超过 80% 时触发。



这意味着警报进入了ALARM说明您的任何数据库在 5 分钟或更长时间内是否出现高 CPU 利用率（超过 80%）。警报仍然在OK说明CPU的利用率是否偶尔在短时间内突增至80%以上，然后再次降至阈值以下。下图说明了这个逻辑。



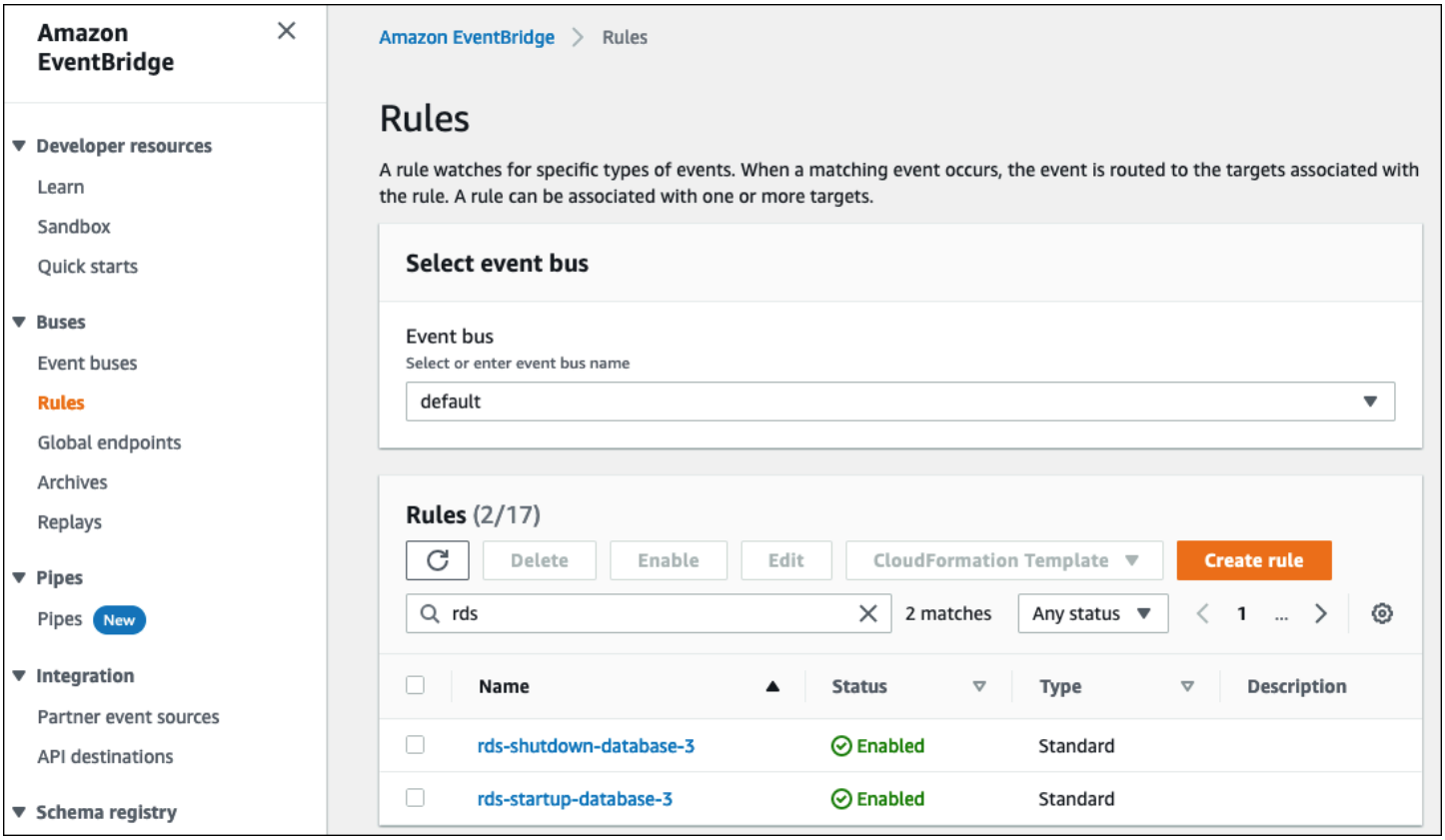
CloudWatch警报支持公制和复合警报。

- 一个指标警报看一首单曲CloudWatch指标，并且可以对指标执行数学表达式。指标警报可以发送 Amazon SNS 消息，反过来，这些消息可以在多个时间段内根据相对于给定阈值的指标值采取一项或多项操作。
- 一个复合警报基于规则表达式，该表达式评估多个警报的状态并输入ALARM仅在满足规则的所有条件时才有状态。复合警报通常用于减少不必要警报的数量。例如，您可能有一个复合警报，其中包含多个指标警报，这些警报配置为从不采取任何操作。当复合警报中的所有单个指标警报都已存在时，复合警报将发送警报ALARM

CloudWatch警报只能观看CloudWatch指标。如果要根据错误、慢速查询或常规日志创建警报，则必须创建CloudWatch来自日志的指标。你可以做到这一点，如前面所述操作系统监控和事件、日志和审计追踪部分，通过使用过滤器来根据日志事件创建指标。同样，要针对增强监控指标发出警报，您必须在中创建指标筛选器CloudWatch从CloudWatch日志。

EventBridge 规则

亚马逊 RDS 活动已配送到亚马逊EventBridge，你可以使用EventBridge规则对这些事件做出反应。例如，你可以创建EventBridge规则将在一个特定的数据库实例停止或启动时通知您并采取操作，如以下屏幕所示。

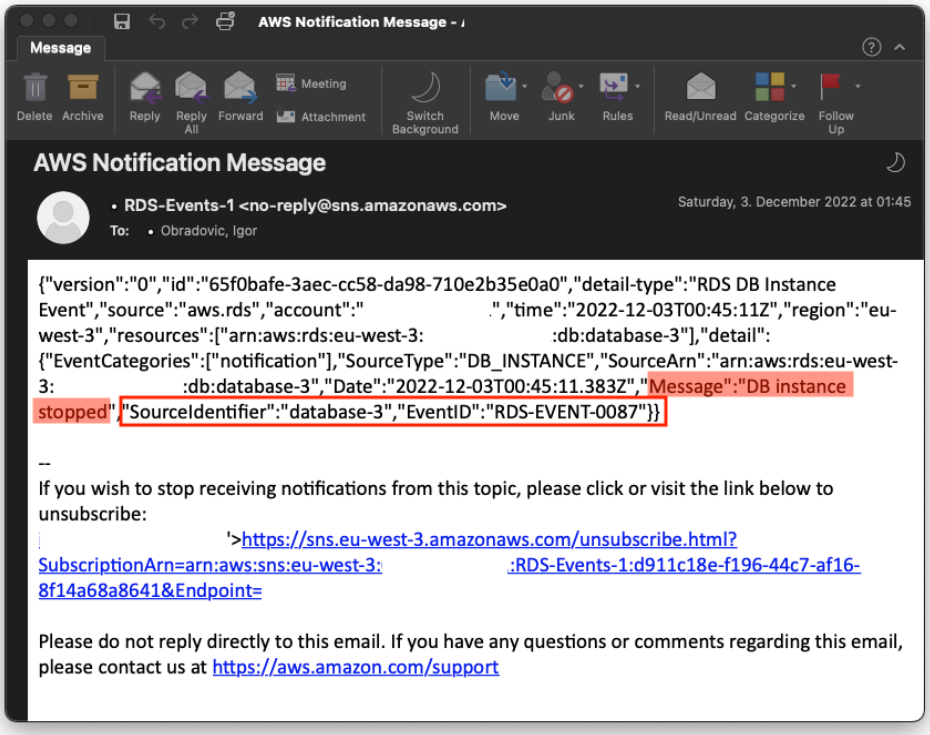


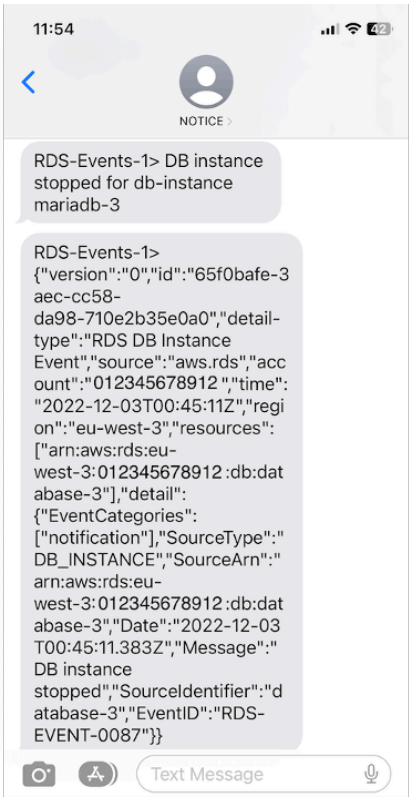
检测规则The DB instance has been stopped事件具有 Amazon RDS 事件 IDRDS-EVENT-0087，所以你设置Event Pattern该规则的属性为：

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

此规则监视数据库实例database-3只有，还有手表RDS-EVENT-0087事件。什么时候EventBridge检测事件，它将事件发送到资源或端点，称为目标。您可以在此处指定在 Amazon RDS 实例关闭

时要采取的操作。您可以将事件发送到许多可能的目标，包括 SNS 主题、亚马逊简单队列服务 (Amazon SQS) 队列和AWS Lambda函数，AWS Systems Manager自动化，AWS Batch任务，亚马逊 API Gateway，事件管理器中的响应计划，一项功能AWS Systems Manager，还有许多其他人。例如，您可以创建一个 SNS 主题，该主题将发送通知电子邮件和 SMS，并将该 SNS 主题指定为目标EventBridge规则。如果 Amazon RDS 数据库实例`database-3`已停止，亚马逊 RDS 发布了该事件`RDS-EVENT-0087`到EventBridge，在那里被检测到。EventBridge然后调用目标，即 SNS 主题。SNS 主题配置为发送电子邮件（如下图所示）和短信。





指定操作、启用和禁用警报

你可以使用CloudWatch警报，用于指定警报在警报之间发生变化时应采取的操作`OK`，`ALARM`，以及`INSUFFICIENT_DATA`各州。CloudWatch内置了与 SNS 主题的集成以及其他几个不适用于 Amazon RDS 指标的操作类别，例如亚马逊弹性计算云 (Amazon EC2) 操作或 Amazon EC2 Auto Scaling 组操作。EventBridge通常用于编写规则和定义在触发 Amazon RDS 指标警报时采取操作的目标。CloudWatch将事件发送到EventBridge每次CloudWatch警报更改其状态。您可以使用这些警报状态更改事件来触发事件目标EventBridge。有关更多信息，请参见警报事件和EventBridge在CloudWatch文档。

您可能还需要管理警报；例如，在计划的配置更改或测试期间自动禁用警报，然后在计划操作结束时重新启用警报。例如，如果您有计划的、有计划的数据库软件升级需要停机，并且您的警报将在数据

库不可用时激活，则可以使用 API 操作禁用和启用警报DisableAlarmActions和EnableAlarmActions，或者disable-alarm-actions和enable-alarm-actions中的命令AWS CLI。您还可以在上查看警报的历史记录CloudWatch控制台或者使用DescribeAlarmHistoryAPI 操作或describe-alarm-history中的命令AWS CLI。CloudWatch将警报历史记录保存两周。在CloudWatch控制台，你可以选择收藏夹和最近导航窗格中的菜单，用于设置和访问您最喜欢的和最近访问的警报。

后续步骤和资源

有关将关系数据库迁移到AWS Cloud，请参阅以下策略AWS规范性指导网站：

- 关系数据库的迁移策略

你可以探索数据库迁移模式为了step-by-step有关在中运行的特定关系数据库的说明AWS Cloud，包括与监控、迁移和数据管理相关的任务。

使用该页面上的过滤器通过以下方式查找模式AWS服务（例如，迁移到 Amazon RDS 或 Amazon Aurora）、按工作负载（例如，开源，包括 MySQL 和 MariaDB 数据库）或按计划用途（生产或试点）划分。

有关其他资源，请参阅以下内容：

- 亚马逊关系数据库服务用户指南
- 亚马逊CloudWatch用户指南
- 亚马逊 RDS 常见问题
- 性能洞察常见问题解答
- 使用 Amazon 向第三方应用程序性能监控服务提供商提供 Amazon RDS 性能洞察计数器指标 CloudWatch指标直播（AWS博客文章）
- 创建亚马逊CloudWatch用于监控亚马逊 RDS 和亚马逊 Aurora MySQL（AWS博客文章）
- 利用性能洞察调整适用于 MySQL 的亚马逊 RD（AWS博客文章）

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
已更新信息	更新了有关导出器的信息，并添加了选择导出器的指南。	2024年6月13日
初次发布	—	2023 年 6 月 30 日

AWS 规范性指导词汇表

以下是 AWS 规范性指导提供的策略、指南和模式中的常用术语。若要推荐词条，请使用术语表末尾的提供反馈链接。

数字

7 R

将应用程序迁移到云中的 7 种常见迁移策略。这些策略以 Gartner 于 2011 年确定的 5 R 为基础，包括以下内容：

- 重构/重新架构 - 充分利用云原生功能来提高敏捷性、性能和可扩展性，以迁移应用程序并修改其架构。这通常涉及到移植操作系统和数据库。示例：将本地 Oracle 数据库迁移到 Amazon Aurora PostgreSQL 兼容版。
- 更换平台 - 将应用程序迁移到云中，并进行一定程度的优化，以利用云功能。示例：将您的本地 Oracle 数据库迁移到 AWS 云端适用于 Oracle 的亚马逊关系数据库服务 (Amazon RDS)。
- 重新购买 - 转换到其他产品，通常是从传统许可转向 SaaS 模式。示例：将客户关系管理（CRM）系统迁移到 Salesforce.com。
- 更换主机（直接迁移）- 将应用程序迁移到云中，无需进行任何更改即可利用云功能。示例：将您的本地 Oracle 数据库迁移到 AWS 云中 EC2 实例上的 Oracle。
- 重新定位（虚拟机监控器级直接迁移）：将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。此迁移场景特定于 VMware Cloud on AWS，它支持虚拟机 (VM) 兼容性和本地环境与之间的工作负载可移植性。 AWS在将基础设施迁移到 VMware Cloud on AWS时，您可以在本地数据中心使用 VMware Cloud Foundation 技术。示例：将托管 Oracle 数据库的虚拟机管理程序重新部署到 VMware Cloud 上。 AWS
- 保留（重访）- 将应用程序保留在源环境中。其中可能包括需要进行重大重构的应用程序，并且您希望将工作推迟到以后，以及您希望保留的遗留应用程序，因为迁移它们没有商业上的理由。
- 停用 - 停用或删除源环境中不再需要的应用程序。

A

ABAC

请参阅基于属性的访问控制。

抽象服务

参见托管服务。

酸

参见原子性、一致性、隔离性、耐久性。

主动-主动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步（通过使用双向复制工具或双写操作），两个数据库都在迁移期间处理来自连接应用程序的事务。这种方法支持小批量、可控的迁移，而不需要一次性割接。与主动-被动迁移相比，它更灵活，但需要更多的工作。

主动-被动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步，但在将数据复制到目标数据库时，只有源数据库处理来自连接应用程序的事务。目标数据库在迁移期间不接受任何事务。

聚合函数

一个 SQL 函数，它对一组行进行操作并计算该组的单个返回值。聚合函数的示例包括SUM和MAX。

AI

参见人工智能。

AIOps

参见人工智能操作。

匿名化

永久删除数据集中个人信息的过程。匿名化可以帮助保护个人隐私。匿名化数据不再被视为个人数据。

反模式

一种用于解决反复出现的问题的常用解决方案，而在这类问题中，此解决方案适得其反、无效或不如替代方案有效。

应用程序控制

一种安全方法，仅允许使用经批准的应用程序，以帮助保护系统免受恶意软件的侵害。

应用程序组合

有关组织使用的每个应用程序的详细信息的集合，包括构建和维护该应用程序的成本及其业务价值。这些信息是产品组合发现和分析过程的关键，有助于识别需要进行迁移、现代化和优化的应用程序并确定其优先级。

人工智能（AI）

计算机科学领域致力于使用计算技术执行通常与人类相关的认知功能，例如学习、解决问题和识别模式。有关更多信息，请参阅什么是人工智能？

人工智能运营（AIOps）

使用机器学习技术解决运营问题、减少运营事故和人为干预以及提高服务质量的过程。有关如何在 AWS 迁移策略中使用 AIOps 的更多信息，请参阅运营集成指南。

非对称加密

一种加密算法，使用一对密钥，一个公钥用于加密，一个私钥用于解密。您可以共享公钥，因为它不用于解密，但对私钥的访问应受到严格限制。

原子性、一致性、隔离性、持久性（ACID）

一组软件属性，即使在出现错误、电源故障或其他问题的情况下，也能保证数据库的数据有效性和操作可靠性。

基于属性的访问权限控制（ABAC）

根据用户属性（如部门、工作角色和团队名称）创建精细访问权限的做法。有关更多信息，请参阅 AWS Identity and Access Management (I AM) 文档 AWS中的 AB AC。

权威数据源

存储主要数据版本的位置，被认为是最可靠的信息源。您可以将数据从权威数据源复制到其他位置，以便处理或修改数据，例如对数据进行匿名化、编辑或假名化。

可用区

中的一个不同位置 AWS 区域 ，不受其他可用区域故障的影响，并向同一区域中的其他可用区提供低成本、低延迟的网络连接。

AWS 云采用框架 (AWS CAF)

该框架包含指导方针和最佳实践 AWS ，可帮助组织制定高效且有效的计划，以成功迁移到云端。AWS CAF将指导分为六个重点领域，称为视角：业务、人员、治理、平台、安全和运营。业务、人员和治理角度侧重于业务技能和流程；平台、安全和运营角度侧重于技术技能和流程。例如，人员角度针对的是负责人力资源（HR）、人员配置职能和人员管理的利益相关者。从这个角度来看，AWS CAF 为人员发展、培训和沟通提供了指导，以帮助组织为成功采用云做好准备。有关更多信息，请参阅 AWS CAF 网站和 AWS CAF 白皮书。

AWS 工作负载资格框架 (AWS WQF)

一种评估数据库迁移工作负载、推荐迁移策略和提供工作估算的工具。 AWS WQF 包含在 AWS Schema Conversion Tool (AWS SCT) 中。它用来分析数据库架构和代码对象、应用程序代码、依赖关系和性能特征，并提供评测报告。

B

坏机器人

旨在破坏个人或组织或对其造成伤害的机器人。

BCP

参见业务连续性计划。

行为图

一段时间内资源行为和交互的统一交互式视图。您可以使用 Amazon Detective 的行为图来检查失败的登录尝试、可疑的 API 调用和类似的操作。有关更多信息，请参阅 Detective 文档中的行为图中的数据。

大端序系统

一个先存储最高有效字节的系统。另请参见字节顺序。

二进制分类

一种预测二进制结果（两个可能的类别之一）的过程。例如，您的 ML 模型可能需要预测诸如“该电子邮件是否为垃圾邮件？”或“这个产品是书还是汽车？”之类的问题

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

蓝/绿部署

一种部署策略，您可以创建两个独立但完全相同的环境。在一个环境中运行当前的应用程序版本（蓝色），在另一个环境中运行新的应用程序版本（绿色）。此策略可帮助您在影响最小的情况下快速回滚。

自动程序

一种通过互联网运行自动任务并模拟人类活动或互动的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的网络爬虫。其他一些被称为恶意机器人的机器人旨在破坏个人或组织或对其造成伤害。

僵尸网络

被恶意软件感染并受单方（称为机器人牧民或机器人操作员）控制的机器人网络。僵尸网络是最著名的扩展机器人及其影响力的机制。

分支

代码存储库的一个包含区域。在存储库中创建的第一个分支是主分支。您可以从现有分支创建新分支，然后在新分支中开发功能或修复错误。为构建功能而创建的分支通常称为功能分支。当功能可以发布时，将功能分支合并回主分支。有关更多信息，请参阅关于分支（GitHub 文档）。

破碎的玻璃通道

在特殊情况下，通过批准的流程，用户 AWS 账户 可以快速访问他们通常没有访问权限的内容。有关更多信息，请参阅 Well -Architected 指南中的 “实施破碎玻璃程序” 指示 AWS 器。

棕地策略

您环境中的现有基础设施。在为系统架构采用棕地策略时，您需要围绕当前系统和基础设施的限制来设计架构。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

企业如何创造价值（例如，销售、客户服务或营销）。微服务架构和开发决策可以由业务能力驱动。有关更多信息，请参阅在 AWS上运行容器化微服务白皮书中的围绕业务能力进行组织部分。

业务连续性计划（BCP）

一项计划，旨在应对大规模迁移等破坏性事件对运营的潜在影响，并使企业能够快速恢复运营。

C

CAF

参见AWS 云采用框架。

金丝雀部署

向最终用户缓慢而渐进地发布版本。当您确信时，可以部署新版本并全部替换当前版本。

CCoE

参见云卓越中心。

CDC

参见变更数据捕获。

更改数据捕获（CDC）

跟踪数据来源（如数据库表）的更改并记录有关更改的元数据的过程。您可以将 CDC 用于各种目的，例如审计或复制目标系统中的更改以保持同步。

混沌工程

故意引入故障或破坏性事件来测试系统的弹性。您可以使用 AWS Fault Injection Service (AWS FIS) 来执行实验，对您的 AWS 工作负载施加压力并评估其响应。

CI/CD

查看持续集成和持续交付。

分类

一种有助于生成预测的分类流程。分类问题的 ML 模型预测离散值。离散值始终彼此不同。例如，一个模型可能需要评估图像中是否有汽车。

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心（CCoE）

一个多学科团队，负责推动整个组织的云采用工作，包括开发云最佳实践、调动资源、制定迁移时间表、领导组织完成大规模转型。有关更多信息，请参阅 AWS 云企业战略博客上的 CCoE 帖子。

云计算

通常用于远程数据存储和 IoT 设备管理的云技术。云计算通常与边缘计算技术相关。

云运营模型

在 IT 组织中，一种用于构建、完善和优化一个或多个云环境的运营模型。有关更多信息，请参阅构建您的云运营模型。

云采用阶段

组织迁移到 AWS 云端时通常要经历的四个阶段：

- 项目 - 出于概念验证和学习目的，开展一些与云相关的项目
- 基础 - 进行基础投资以扩大云采用率（例如，创建登录区、定义 CCoE、建立运营模型）
- 迁移 - 迁移单个应用程序

- 重塑 - 优化产品和服务，在云中创新

Stephen Orban 在 “云企业战略” 博客文章《云优先之旅和采用阶段》中定义了 AWS 这些阶段。有关它们与 AWS 迁移策略的关系的信息，请参阅迁移准备指南。

CMDB

参见配置管理数据库。

代码存储库

通过版本控制过程存储和更新源代码和其他资产（如文档、示例和脚本）的位置。常见的云存储库包括 GitHub 或 AWS CodeCommit。每个版本的代码都称为一个分支。在微服务结构中，每个存储库都专门用于一个功能。单个 CI/CD 管道可以使用多个存储库。

冷缓存

一种空的、填充不足或包含过时或不相关数据的缓冲区缓存。这会影响性能，因为数据库实例必须从主内存或磁盘读取，这比从缓冲区缓存读取要慢。

冷数据

很少访问的数据，且通常是历史数据。查询此类数据时，通常可以接受慢速查询。将这些数据转移到性能较低且成本更低的存储层或类别可以降低成本。

计算机视觉 (CV)

人工智能领域，使用机器学习来分析和提取数字图像和视频等视觉格式的信息。例如，AWS Panorama 提供将 CV 添加到本地摄像机网络的设备，而 Amazon 则为 CV SageMaker 提供图像处理算法。

配置偏差

对于工作负载，配置会从预期状态发生变化。这可能会导致工作负载变得不合规，而且通常是渐进的，不是故意的。

配置管理数据库（CMDB）

一种存储库，用于存储和管理有关数据库及其 IT 环境的信息，包括硬件和软件组件及其配置。您通常在迁移的产品组合发现和分析阶段使用来自 CMDB 的数据。

合规性包

一系列 AWS Config 规则和补救措施，您可以汇编这些规则和补救措施，以自定义合规性和安全性检查。您可以使用 YAML 模板将一致性包作为单个实体部署在 AWS 账户 和区域或整个组织中。有关更多信息，请参阅 AWS Config 文档中的一致性包。

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。CI/CD 通常被描述为管道。CI/CD 可以帮助您实现流程自动化、提高工作效率、改善代码质量并加快交付速度。有关更多信息，请参阅持续交付的优势。CD 也可以表示持续部署。有关更多信息，请参阅持续交付与持续部署。

CV

参见计算机视觉。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 Well-Architecte AWS d Framework 中安全支柱的一个组成部分。有关详细信息，请参阅数据分类。

数据漂移

生产数据与用来训练机器学习模型的数据之间的有意义差异，或者输入数据随时间推移的有意义变化。数据漂移可能降低机器学习模型预测的整体质量、准确性和公平性。

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据网格

一种架构框架，可提供分布式、去中心化的数据所有权以及集中式管理和治理。

数据最少化

仅收集并处理绝对必要数据的原则。在中进行数据最小化 AWS Cloud 可以降低隐私风险、成本和分析碳足迹。

数据边界

AWS 环境中的一组预防性防护措施，可帮助确保只有可信身份才能访问来自预期网络的可信资源。有关更多信息，请参阅在上构建数据边界。 AWS

数据预处理

将原始数据转换为 ML 模型易于解析的格式。预处理数据可能意味着删除某些列或行，并处理缺失、不一致或重复的值。

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

一种支持商业智能（例如分析）的数据管理系统。数据仓库通常包含大量历史数据，通常用于查询和分析。

数据库定义语言（DDL）

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言（DML）

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

参见数据库定义语言。

深度融合

组合多个深度学习模型进行预测。您可以使用深度融合来获得更准确的预测或估算预测中的不确定性。

深度学习

一个 ML 子字段使用多层人工神经网络来识别输入数据和感兴趣的目标变量之间的映射。

defense-in-depth

一种信息安全方法，经过深思熟虑，在整个计算机网络中分层实施一系列安全机制和控制措施，以保护网络及其中数据的机密性、完整性和可用性。当你采用这种策略时 AWS，你会在 AWS Organizations 结构的不同层面添加多个控件来帮助保护资源。例如，一种 defense-in-depth 方法可以结合多因素身份验证、网络分段和加密。

委托管理员

在中 AWS Organizations，兼容的服务可以注册 AWS 成员帐户来管理组织的帐户并管理该服务的权限。此账户被称为该服务的委托管理员。有关更多信息和兼容服务列表，请参阅 AWS Organizations 文档中使用 AWS Organizations的服务。

部署

使应用程序、新功能或代码修复在目标环境中可用的过程。部署涉及在代码库中实现更改，然后在应用程序的环境中构建和运行该代码库。

开发环境

参见环境。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出警报。这些控制是第二道防线，提醒您注意绕过现有预防性控制的安全事件。有关更多信息，请参阅在 AWS上实施安全控制中的侦测性控制。

开发价值流映射 (DVSM)

用于识别对软件开发生命周期中的速度和质量产生不利影响的限制因素并确定其优先级的流程。DVSM 扩展了最初为精益生产实践设计的价值流映射流程。其重点关注在软件开发过程中创造和转移价值所需的步骤和团队。

数字孪生

真实世界系统的虚拟再现，如建筑物、工厂、工业设备或生产线。数字孪生支持预测性维护、远程监控和生产优化。

维度表

在星型架构中，一种较小的表，其中包含事实表中定量数据的数据属性。维度表属性通常是文本字段或行为类似于文本的离散数字。这些属性通常用于查询约束、筛选和结果集标注。

灾难

阻止工作负载或系统在其主要部署位置实现其业务目标的事件。这些事件可能是自然灾害、技术故障或人为操作的结果，例如无意的配置错误或恶意软件攻击。

灾难恢复 (DR)

您用来最大限度地减少灾难造成的停机时间和数据丢失的策略和流程。有关更多信息，请参阅 Well-Architected Fr ame AWS work 中的 “工作负载灾难恢复：云端 AWS 恢复”。

DML

参见数据库操作语言。

领域驱动设计

一种开发复杂软件系统的方法，通过将其组件连接到每个组件所服务的不断发展的领域或核心业务目标。Eric Evans 在其著作领域驱动设计：软件核心复杂性应对之道（Boston: Addison-Wesley Professional, 2003）中介绍了这一概念。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

参见灾难恢复。

漂移检测

跟踪与基准配置的偏差。例如，您可以使用 AWS CloudFormation 来检测系统资源中的偏差，也可以使用 AWS Control Tower 来检测着陆区中可能影响监管要求合规性的变化。

DVSM

参见开发价值流映射。

E

EDA

参见探索性数据分析。

边缘计算

该技术可提高位于 IoT 网络边缘的智能设备的计算能力。与云计算相比，边缘计算可以减少通信延迟并缩短响应时间。

加密

一种将人类可读的纯文本数据转换为密文的计算过程。

加密密钥

由加密算法生成的随机位的加密字符串。密钥的长度可能有所不同，而且每个密钥都设计为不可预测且唯一。

字节顺序

字节在计算机内存中的存储顺序。大端序系统先存储最高有效字节。小端序系统先存储最低有效字节。

端点

参见服务端点。

端点服务

一种可以在虚拟私有云（VPC）中托管，与其他用户共享的服务。您可以使用其他 AWS 账户 或 AWS Identity and Access Management (IAM) 委托人创建终端节点服务， AWS PrivateLink 并向其授予权限。这些账户或主体可通过创建接口 VPC 端点来私密地连接到您的端点服务。有关更多信息，请参阅 Amazon Virtual Private Cloud（Amazon VPC）文档中的创建端点服务。

企业资源规划 (ERP)

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

用另一个加密密钥对加密密钥进行加密的过程。有关更多信息，请参阅 AWS Key Management Service (AWS KMS) 文档中的信封加密。

environment

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

- 开发环境 — 正在运行的应用程序的实例，只有负责维护应用程序的核心团队才能使用。开发环境用于测试更改，然后再将其提升到上层环境。这类环境有时称为测试环境。
- 下层环境 — 应用程序的所有开发环境，比如用于初始构建和测试的环境。
- 生产环境 — 最终用户可以访问的正在运行的应用程序的实例。在 CI/CD 管道中，生产环境是最后一个部署环境。
- 上层环境 — 除核心开发团队以外的用户可以访问的所有环境。这可能包括生产环境、预生产环境和用户验收测试环境。

epic

在敏捷方法学中，有助于组织工作和确定优先级的功能类别。epics 提供了对需求和实施任务的总体描述。例如， AWS CAF 安全史诗包括身份和访问管理、侦探控制、基础设施安全、数据保护和事件响应。有关 AWS 迁移策略中 epics 的更多信息，请参阅计划实施指南。

ERP

参见企业资源规划。

探索性数据分析（EDA）

分析数据集以了解其主要特征的过程。您收集或汇总数据，并进行初步调查，以发现模式、检测异常并检查假定情况。EDA 通过计算汇总统计数据和创建数据可视化得以执行。

F

事实表

星形架构中的中心表。它存储有关业务运营的定量数据。通常，事实表包含两种类型的列：包含度量的列和包含维度表外键的列。

失败得很快

一种使用频繁和增量测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

在中 AWS Cloud，诸如可用区 AWS 区域、控制平面或数据平面之类的边界，它限制了故障的影响并有助于提高工作负载的弹性。有关更多信息，请参阅AWS 故障隔离边界。

功能分支

参见分支。

特征

您用来进行预测的输入数据。例如，在制造环境中，特征可能是定期从生产线捕获的图像。

特征重要性

特征对于模型预测的重要性。这通常表示为数值分数，可以通过各种技术进行计算，例如 Shapley 加法解释（SHAP）和积分梯度。有关更多信息，请参阅机器学习模型的可解释性：AWS。

功能转换

为 ML 流程优化数据，包括使用其他来源丰富数据、扩展值或从单个数据字段中提取多组信息。这使得 ML 模型能从数据中获益。例如，如果您将“2021-05-27 00:15:37”日期分解为“2021”、“五月”、“星期四”和“15”，则可以帮助学习与不同数据成分相关的算法学习精细模式。

FGAC

请参阅精细的访问控制。

精细访问控制 (FGAC)

使用多个条件允许或拒绝访问请求。

快闪迁移

一种数据库迁移方法，它使用连续的数据复制，通过更改数据捕获在尽可能短的时间内迁移数据，而不是使用分阶段的方法。目标是将停机时间降至最低。

G

地理封锁

请参阅地理限制。

地理限制（地理阻止）

在 Amazon 中 CloudFront，一种阻止特定国家/地区的用户访问内容分发的选项。您可以使用允许列表或阻止列表来指定已批准和已禁止的国家/地区。有关更多信息，请参阅 CloudFront 文档中的限制内容的地理分布。

GitFlow 工作流程

一种方法，在这种方法中，下层和上层环境在源代码存储库中使用不同的分支。Gitflow 工作流程被认为是传统的，而基于主干的工作流程是现代的首选方法。

全新策略

在新环境中缺少现有基础设施。在对系统架构采用全新策略时，您可以选择所有新技术，而不受对现有基础设施（也称为棕地）兼容性的限制。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

防护机制

一种高级规则，用于跨组织单位（OU）管理资源、策略和合规性。预防性防护机制会执行策略以确保符合合规性标准。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性防护机制会检测策略违规和合规性问题，并生成警报以进行修复。它们通过使用 AWS Config、、Amazon、 AWS Security Hub GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

H

HA

参见高可用性。

异构数据库迁移

将源数据库迁移到使用不同数据库引擎的目标数据库（例如，从 Oracle 迁移到 Amazon Aurora）。异构迁移通常是重新架构工作的一部分，而转换架构可能是一项复杂的任务。AWS 提供了 AWS SCT 来帮助实现架构转换。

高可用性 (HA)

在遇到挑战或灾难时，工作负载无需干预即可连续运行的能力。HA 系统旨在自动进行故障转移、持续提供良好性能，并以最小的性能影响处理不同负载和故障。

历史数据库现代化

一种用于实现运营技术 (OT) 系统现代化和升级以更好满足制造业需求的方法。历史数据库是一种用于收集和存储工厂中各种来源数据的数据库。

同构数据库迁移

将源数据库迁移到共享同一数据库引擎的目标数据库（例如，从 Microsoft SQL Server 迁移到 Amazon RDS for SQL Server）。同构迁移通常是更换主机或更换平台工作的一部分。您可以使用本机数据库实用程序来迁移架构。

热数据

经常访问的数据，例如实时数据或近期的转化数据。这些数据通常需要高性能存储层或存储类别才能提供快速的查询响应。

修补程序

针对生产环境中关键问题的紧急修复。由于其紧迫性，修补程序通常是在典型的 DevOps 发布工作流程之外进行的。

hypercare 周期

割接之后，迁移团队立即管理和监控云中迁移的应用程序以解决任何问题的时间段。通常，这个周期持续 1-4 天。在 hypercare 周期结束时，迁移团队通常会将应用程序的责任移交给云运营团队。

I

IaC

参见基础架构即代码。

基于身份的策略

附加到一个或多个 IAM 委托人的策略，用于定义他们在 AWS Cloud 环境中的权限。

空闲应用程序

90 天内平均 CPU 和内存使用率在 5% 到 20% 之间的应用程序。在迁移项目中，通常会停用这些应用程序或将其保留在本地。

IIoT

参见工业物联网。

不可变的基础架构

一种为生产工作负载部署新基础架构，而不是更新、修补或修改现有基础架构的模型。不可变基础架构本质上比可变基础架构更一致、更可靠、更可预测。有关更多信息，请参阅 Well-Architected Framework 中的使用不可变基础架构 AWS 部署最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，一种接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

增量迁移

一种割接策略，在这种策略中，您可以将应用程序分成小部分进行迁移，而不是一次性完整割接。例如，您最初可能只将几个微服务或用户迁移到新系统。在确认一切正常后，您可以逐步迁移其他微服务或用户，直到停用遗留系统。这种策略降低了大规模迁移带来的风险。

工业 4.0

该术语由克劳斯·施瓦布（Klaus Schwab）于2016年推出，指的是通过连接、实时数据、自动化、分析和人工智能/机器学习的进步实现制造流程的现代化。

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

通过一组配置文件预置和管理应用程序基础设施的过程。IaC 旨在帮助您集中管理基础设施、实现资源标准化和快速扩展，使新环境具有可重复性、可靠性和一致性。

工业物联网（IIoT）

在工业领域使用联网的传感器和设备，例如制造业、能源、汽车、医疗保健、生命科学和农业。有关更多信息，请参阅制定工业物联网（IIoT）数字化转型策略。

检查 VPC

在 AWS 多账户架构中，一种集中式 VPC，用于管理 VPC（相同或不同 AWS 区域）、互联网和本地网络之间的网络流量检查。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

物联网（IoT）

由带有嵌入式传感器或处理器的连接物理对象组成的网络，这些传感器或处理器通过互联网或本地通信网络与其他设备和系统进行通信。有关更多信息，请参阅什么是 IoT？

可解释性

它是机器学习模型的一种特征，描述了人类可以理解模型的预测如何取决于其输入的程度。有关更多信息，请参阅使用 AWS 实现机器学习模型的可解释性。

IoT

参见物联网。

IT 信息库（ITIL）

提供 IT 服务并使这些服务符合业务要求的一套最佳实践。ITIL 是 ITSM 的基础。

IT 服务管理（ITSM）

为组织设计、实施、管理和支持 IT 服务的相关活动。有关将云运营与 ITSM 工具集成的信息，请参阅运营集成指南。

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

L

基于标签的访问控制 (LBAC)

强制访问控制 (MAC) 的一种实施方式，其中明确为用户和数据本身分配了安全标签值。用户安全标签和数据安全标签之间的交集决定了用户可以看到哪些行和列。

登录区

landing zone 是一个架构精良的多账户 AWS 环境，具有可扩展性和安全性。这是一个起点，您的组织可以从这里放心地在安全和基础设施环境中快速启动和部署工作负载和应用程序。有关登录区的更多信息，请参阅设置安全且可扩展的多账户 AWS 环境。

大规模迁移

迁移 300 台或更多服务器。

LBAC

参见基于标签的访问控制。

最低权限

授予执行任务所需的最低权限的最佳安全实践。有关更多信息，请参阅 IAM 文档中的应用最低权限许可。

直接迁移

见 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参见字节顺序。

下层环境

参见环境。

M

机器学习（ML）

一种使用算法和技术进行模式识别和学习的人工智能。ML 对记录的数据（例如物联网（IoT）数据）进行分析和学习，以生成基于模式的统计模型。有关更多信息，请参阅机器学习。

主分支

参见分支。

恶意软件

旨在危害计算机安全或隐私的软件。恶意软件可能会破坏计算机系统、泄露敏感信息或获得未经授权的访问。恶意软件的示例包括病毒、蠕虫、勒索软件、特洛伊木马、间谍软件和键盘记录器。

托管服务

AWS 服务 它 AWS 运行基础设施层、操作系统和平台，您可以访问端点来存储和检索数据。亚马逊简单存储服务 (Amazon S3) Service 和 Amazon DynamoDB 就是托管服务的示例。这些服务也称为抽象服务。

制造执行系统 (MES)

一种软件系统，用于跟踪、监控、记录和控制在车间将原材料转化为成品的生产过程。

MAP

参见迁移加速计划。

机制

一个完整的过程，在此过程中，您可以创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运行过程中自我增强和改进的循环。有关更多信息，请参阅在 Well-Architect AWS ed 框架中构建机制。

成员账户

AWS 账户 除属于组织中的管理账户之外的所有账户 AWS Organizations。一个账户一次只能是一个组织的成员。

MES

参见制造执行系统。

消息队列遥测传输 (MQTT)

一种基于发布/订阅模式的轻量级 machine-to-machine (M2M) 通信协议，适用于资源受限的物联网设备。

微服务

一种小型独立服务，通过明确定义的 API 进行通信，通常由小型独立团队拥有。例如，保险系统可能包括映射到业务能力（如销售或营销）或子域（如购买、理赔或分析）的微服务。微服务的好处包括敏捷、灵活扩展、易于部署、可重复使用的代码和恢复能力。有关更多信息，请参阅使用 AWS 无服务器服务集成微服务。

微服务架构

一种使用独立组件构建应用程序的方法，这些组件将每个应用程序进程作为微服务运行。这些微服务使用轻量级 API 通过明确定义的接口进行通信。该架构中的每个微服务都可以更新、部署和扩展，以满足对应用程序特定功能的需求。有关更多信息，请参阅在上实现微服务。 AWS

迁移加速计划（MAP）

AWS 该计划提供咨询支持、培训和服务，以帮助组织为迁移到云奠定坚实的运营基础，并帮助抵消迁移的初始成本。MAP 提供了一种以系统的方式执行遗留迁移的迁移方法，以及一套用于自动执行和加速常见迁移场景的工具。

大规模迁移

将大部分应用程序组合分波迁移到云中的过程，在每一波中以更快的速度迁移更多应用程序。本阶段使用从早期阶段获得的最佳实践和经验教训，实施由团队、工具和流程组成的迁移工厂，通过自动化和敏捷交付简化工作负载的迁移。这是 AWS 迁移策略的第三阶段。

迁移工厂

跨职能团队，通过自动化、敏捷的方法简化工作负载迁移。迁移工厂团队通常包括运营、业务分析师和所有者、迁移工程师、开发 DevOps 人员和冲刺专业人员。20% 到 50% 的企业应用程序组合由可通过工厂方法优化的重复模式组成。有关更多信息，请参阅本内容集中有关迁移工厂的讨论和云迁移工厂指南。

迁移元数据

有关完成迁移所需的应用程序和服务器的信息。每种迁移模式都需要一套不同的迁移元数据。迁移元数据的示例包括目标子网、安全组和 AWS 账户。

迁移模式

一种可重复的迁移任务，详细列出了迁移策略、迁移目标以及所使用的迁移应用程序或服务。示例：使用 AWS 应用程序迁移服务重新托管向 Amazon EC2 的迁移。

迁移组合评测（MPA）

一种在线工具，可提供信息，用于验证迁移到 AWS 云端的业务案例。MPA 提供了详细的组合评测（服务器规模调整、定价、TCO 比较、迁移成本分析）以及迁移计划（应用程序数据分析和数据收集、应用程序分组、迁移优先级排序和波次规划）。所有 AWS 顾问和 APN 合作伙伴顾问均可免费使用 MPA 工具（需要登录）。

迁移准备情况评测（MRA）

使用 AWS CAF 深入了解组织的云就绪状态、确定优势和劣势以及制定行动计划以缩小已发现差距的过程。有关更多信息，请参阅迁移准备指南。MRA 是 AWS 迁移策略的第一阶段。

迁移策略

用于将工作负载迁移到 AWS 云端的方法。有关更多信息，请参阅此词汇表中的 7 R 条目和动员组织以加快大规模迁移。

ML

参见机器学习。

现代化

将过时的（原有的或单体）应用程序及其基础设施转变为云中敏捷、弹性和高度可用的系统，以降低成本、提高效率和利用创新。有关更多信息，请参阅中的应用程序现代化策略。 AWS Cloud

现代化准备情况评估

一种评估方式，有助于确定组织应用程序的现代化准备情况；确定收益、风险和依赖关系；确定组织能够在多大程度上支持这些应用程序的未来状态。评估结果是目标架构的蓝图、详细说明现代化进程发展阶段和里程碑的路线图以及解决已发现差距的行动计划。有关详细信息，请参阅在 AWS 云中评估应用程序的现代化准备情况。

单体应用程序（单体式）

作为具有紧密耦合进程的单个服务运行的应用程序。单体应用程序有几个缺点。如果某个应用程序功能的需求激增，则必须扩展整个架构。随着代码库的增长，添加或改进单体应用程序的功能也会变得更加复杂。若要解决这些问题，可以使用微服务架构。有关更多信息，请参阅将单体分解为微服务。

MPA

参见迁移组合评估。

MQTT

请参阅消息队列遥测传输。

多分类器

一种帮助为多个类别生成预测（预测两个以上结果之一）的过程。例如，ML 模型可能会询问“这个产品是书、汽车还是手机？”或“此客户最感兴趣什么类别的产品？”

可变基础架构

一种用于更新和修改现有生产工作负载基础架构的模型。为了提高一致性、可靠性和可预测性，Well-Architect AWS ed Framework 建议使用不可变基础设施作为最佳实践。

O

OAC

请参阅源站访问控制。

OAI

参见源访问身份。

OCM

参见组织变更管理。

离线迁移

一种迁移方法，在这种方法中，源工作负载会在迁移过程中停止运行。这种方法会延长停机时间，通常用于小型非关键工作负载。

OI

参见运营集成。

OLA

参见运营层协议。

在线迁移

一种迁移方法，在这种方法中，源工作负载无需离线即可复制到目标系统。在迁移过程中，连接工作负载的应用程序可以继续运行。这种方法的停机时间为零或最短，通常用于关键生产工作负载。

OPC-UA

参见开放流程通信-统一架构。

开放流程通信-统一架构 (OPC-UA)

一种用于工业自动化的 machine-to-machine （M2M）通信协议。OPC-UA 提供了数据加密、身份验证和授权方案的互操作性标准。

运营级别协议（OLA）

一项协议，阐明了 IT 职能部门承诺相互交付的内容，以支持服务水平协议（SLA）。

运营准备情况审查 (ORR)

一份问题清单和相关的最佳实践，可帮助您理解、评估、预防或缩小事件和可能的故障的范围。有关更多信息，请参阅 Well-Architecte AWS d Frame work 中的运营准备情况评估 (ORR)。

操作技术 (OT)

与物理环境配合使用以控制工业运营、设备和基础设施的硬件和软件系统。在制造业中，OT 和信息技术 (IT) 系统的集成是工业 4.0 转型的重点。

运营整合（OI）

在云中实现运营现代化的过程，包括就绪计划、自动化和集成。有关更多信息，请参阅运营整合指南。

组织跟踪

由 AWS CloudTrail 此创建的跟踪记录组织 AWS 账户 中所有人的所有事件 AWS Organizations。该跟踪是在每个 AWS 账户 中创建的，属于组织的一部分，并跟踪每个账户的活动。有关更多信息，请参阅 CloudTrail文档中的为组织创建跟踪。

组织变革管理（OCM）

一个从人员、文化和领导力角度管理重大、颠覆性业务转型的框架。OCM 通过加快变革采用、解决过渡问题以及推动文化和组织变革，帮助组织为新系统和战略做好准备和过渡。在 AWS 迁移策略中，该框架被称为人员加速，因为云采用项目需要变更的速度。有关更多信息，请参阅 OCM 指南。

来源访问控制（OAC）

中 CloudFront，一个增强的选项，用于限制访问以保护您的亚马逊简单存储服务 (Amazon S3) 内容。OAC 全部支持所有 S3 存储桶 AWS 区域、使用 AWS KMS (SSE-KMS) 进行服务器端加密，以及对 S3 存储桶的动态PUT和DELETE请求。

来源访问身份（OAI）

在中 CloudFront，一个用于限制访问权限以保护您的 Amazon S3 内容的选项。当您使用 OAI 时，CloudFront 会创建一个 Amazon S3 可以对其进行身份验证的委托人。经过身份验证的委托人只能通过特定 CloudFront 分配访问 S3 存储桶中的内容。另请参阅 OAC，其中提供了更精细和增强的访问控制。

或者

参见运营准备情况审查。

OT

参见运营技术。

出站（出口）VPC

在 AWS 多账户架构中，一种处理从应用程序内部启动的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

P

权限边界

附加到 IAM 主体的 IAM 管理策略，用于设置用户或角色可以拥有的最大权限。有关更多信息，请参阅 IAM 文档中的权限边界。

个人身份信息 (PII)

直接查看其他相关数据或与之配对时可用于合理推断个人身份的信息。PII 的示例包括姓名、地址和联系信息。

PII

查看个人身份信息。

playbook

一套预定义的步骤，用于捕获与迁移相关的工作，例如在云中交付核心运营功能。playbook 可以采用脚本、自动化运行手册的形式，也可以是操作现代化环境所需的流程或步骤的摘要。

PLC

参见可编程逻辑控制器。

PLM

参见产品生命周期管理。

策略

一个对象，可以在中定义权限（参见基于身份的策略）、指定访问条件（参见基于资源的策略）或定义组织中所有账户的最大权限 AWS Organizations （参见服务控制策略）。

多语言持久性

根据数据访问模式和其他要求，独立选择微服务的数据存储技术。如果您的微服务采用相同的数据存储技术，它们可能会遇到实现难题或性能不佳。如果微服务使用最适合其需求的数据存储，则可以更轻松地实现微服务，并获得更好的性能和可扩展性。有关更多信息，请参阅在微服务中实现数据持久性。

组合评测

一个发现、分析和确定应用程序组合优先级以规划迁移的过程。有关更多信息，请参阅评估迁移准备情况。

谓词

返回`true`或的查询条件`false`，通常位于子`WHERE`句中。

谓词下推

一种数据库查询优化技术，可在传输前筛选查询中的数据。这减少了必须从关系数据库检索和处理的数据量，并提高了查询性能。

预防性控制

一种安全控制，旨在防止事件发生。这些控制是第一道防线，帮助防止未经授权的访问或对网络的意外更改。有关更多信息，请参阅在 AWS上实施安全控制中的预防性控制。

主体

中 AWS 可以执行操作和访问资源的实体。此实体通常是 IAM 角色的根用户或用户。 AWS 账户有关更多信息，请参阅 IAM 文档中角色术语和概念中的主体。

隐私设计

一种贯穿整个工程化过程考虑隐私的系统工程方法。

私有托管区

私有托管区就是一个容器，其中包含的信息说明您希望 Amazon Route 53 如何响应一个或多个 VPC 中的某个域及其子域的 DNS 查询。有关更多信息，请参阅 Route 53 文档中的私有托管区的使用。

主动控制

一种安全控制措施，旨在防止部署不合规的资源。这些控件会在资源配置之前对其进行扫描。如果资源与控件不兼容，则不会对其进行配置。有关更多信息，请参阅 AWS Control Tower 文档中的控制参考指南，并参见在上实施安全控制中的主动控制 AWS。

产品生命周期管理 (PLM)

在产品的整个生命周期中，从设计、开发和上市，到成长和成熟，再到衰落和移除，对产品进行数据和流程的管理。

生产环境

参见环境。

可编程逻辑控制器 (PLC)

在制造业中，一种高度可靠、适应性强的计算机，用于监控机器并实现制造过程自动化。

假名化

用占位符值替换数据集中个人标识符的过程。假名化可以帮助保护个人隐私。假名化数据仍被视为个人数据。

发布/订阅（发布/订阅）

一种支持微服务间异步通信的模式，以提高可扩展性和响应能力。例如，在基于微服务的 MES 中，微服务可以将事件消息发布到其他微服务可以订阅的频道。系统可以在不更改发布服务的情况下添加新的微服务。

Q

查询计划

一系列步骤，例如指令，用于访问 SQL 关系数据库系统中的数据。

查询计划回归

当数据库服务优化程序选择的最佳计划不如数据库环境发生特定变化之前时。这可能是由统计数据、约束、环境设置、查询参数绑定更改和数据库引擎更新造成的。

R

RACI 矩阵

参见负责任、负责、咨询、知情（RACI）。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

参见负责任、负责、咨询、知情（RACI）。

RCAC

请参阅行和列访问控制。

只读副本

用于只读目的的数据库副本。您可以将查询路由到只读副本，以减轻主数据库的负载。

重新架构师

见 7 R。

恢复点目标 (RPO)

自上一个数据恢复点以来可接受的最长时间。这决定了从上一个恢复点到服务中断之间可接受的数据丢失情况。

恢复时间目标 (RTO)

服务中断和服务恢复之间可接受的最大延迟。

重构

见 7 R。

区域

地理区域内的 AWS 资源集合。每一个 AWS 区域 都相互隔离，彼此独立，以提供容错、稳定性和弹性。有关更多信息，请参阅指定 AWS 区域 您的账户可以使用的账户。

回归

一种预测数值的 ML 技术。例如，要解决“这套房子的售价是多少？”的问题 ML 模型可以使用线性回归模型，根据房屋的已知事实（如建筑面积）来预测房屋的销售价格。

重新托管

见 7 R。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 7 R。

更换平台

见 7 R。

回购

见 7 R。

故障恢复能力

应用程序抵御中断或从中断中恢复的能力。在中规划弹性时，高可用性和灾难恢复是常见的考虑因素。 AWS Cloud有关更多信息，请参阅AWS Cloud 弹性。

基于资源的策略

一种附加到资源的策略，例如 AmazonS3 存储桶、端点或加密密钥。此类策略指定了允许哪些主体访问、支持的操作以及必须满足的任何其他条件。

责任、问责、咨询和知情（RACI）矩阵

定义参与迁移活动和云运营的所有各方的角色和责任的矩阵。矩阵名称源自矩阵中定义的责任类型：负责 (R)、问责 (A)、咨询 (C) 和知情 (I)。支持 (S) 类型是可选的。如果包括支持，则该矩阵称为 RASCI 矩阵，如果将其排除在外，则称为 RACI 矩阵。

响应性控制

一种安全控制，旨在推动对不良事件或偏离安全基线的情况进行修复。有关更多信息，请参阅在AWS上实施安全控制中的响应性控制。

保留

见 7 R。

退休

见 7 R。

旋转

定期更新密钥以使攻击者更难访问凭据的过程。

行列访问控制 (RCAC)

使用已定义访问规则的基本、灵活的 SQL 表达式。RCAC 由行权限和列掩码组成。

RPO

参见恢复点目标。

RTO

参见恢复时间目标。

运行手册

执行特定任务所需的一套手动或自动程序。它们通常是为了简化重复性操作或高错误率的程序而设计的。

S

SAML 2.0

许多身份提供商 (IdPs) 使用的开放标准。此功能支持联合单点登录 (SSO)，因此用户无需在 IAM 中为组织中的所有人创建用户即可登录 AWS Management Console 或调用 AWS API 操作。有关基于 SAML 2.0 的联合身份验证的更多信息，请参阅 IAM 文档中的关于基于 SAML 2.0 的联合身份验证。

SCADA

参见监督控制和数据采集。

SCP

参见服务控制政策。

secret

在中 AWS Secrets Manager，您以加密形式存储的机密或受限信息，例如密码或用户凭证。它由密钥值及其元数据组成。密钥值可以是二进制、单个字符串或多个字符串。有关更多信息，请参阅 Sec rets Manager 文档中的密钥。

安全控制

一种技术或管理防护机制，可防止、检测或降低威胁行为体利用安全漏洞的能力。安全控制主要有四种类型：预防性、侦测、响应式和主动式。

安全加固

缩小攻击面，使其更能抵御攻击的过程。这可能包括删除不再需要的资源、实施授予最低权限的最佳安全实践或停用配置文件中不必要的功能等操作。

安全信息和事件管理（SIEM）系统

结合了安全信息管理（SIM）和安全事件管理（SEM）系统的工具和服务。SIEM 系统会收集、监控和分析来自服务器、网络、设备和其他来源的数据，以检测威胁和安全漏洞，并生成警报。

安全响应自动化

一种预定义和编程的操作，旨在自动响应或修复安全事件。这些自动化可作为侦探或响应式安全控制措施，帮助您实施 AWS 安全最佳实践。自动响应操作的示例包括修改 VPC 安全组、修补 Amazon EC2 实例或轮换证书。

服务器端加密

由接收数据的人在目的地对数据 AWS 服务 进行加密。

服务控制策略（SCP）

一种策略，用于集中控制 AWS Organizations的组织中所有账户的权限。SCP 为管理员可以委托给用户或角色的操作定义了防护机制或设定了限制。您可以将 SCP 用作允许列表或拒绝列表，指定允许或禁止哪些服务或操作。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略。

服务端点

的入口点的 URL AWS 服务。您可以使用端点，通过编程方式连接到目标服务。有关更多信息，请参阅 AWS 一般参考 中的 AWS 服务 端点。

服务水平协议（SLA）

一份协议，阐明了 IT 团队承诺向客户交付的内容，比如服务正常运行时间和性能。

服务级别指示器 (SLI)

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 (SLO)

代表服务运行状况的目标指标，由服务级别指标衡量。

责任共担模式

描述您在云安全与合规方面共同承担 AWS 的责任的模型。 AWS 负责云的安全，而您则负责云中的安全。有关更多信息，请参阅责任共担模式。

暹粒

参见安全信息和事件管理系统。

单点故障 (SPOF)

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

参见服务级别协议。

SLI

参见服务级别指标。

SLO

参见服务级别目标。

split-and-seed 模型

一种扩展和加速现代化项目的模式。随着新功能和产品发布的定义，核心团队会拆分以创建新的产品团队。这有助于扩展组织的能力和服务，提高开发人员的工作效率，支持快速创新。有关更多信息，请参阅中的分阶段实现应用程序现代化的方法。 AWS Cloud

恶作剧

参见单点故障。

星型架构

一种数据库组织结构，它使用一个大型事实表来存储交易数据或测量数据，并使用一个或多个较小的维度表来存储数据属性。此结构专为在数据仓库中使用或用于商业智能目的而设计。

strangler fig 模式

一种通过逐步重写和替换系统功能直至可以停用原有的系统来实现单体系统现代化的方法。这种模式用无花果藤作为类比，这种藤蔓成长为一棵树，最终战胜并取代了宿主。该模式是由 Martin Fowler 提出的，作为重写单体系统时管理风险的一种方法。有关如何应用此模式的示例，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监控和数据采集 (SCADA)

在制造业中，一种使用硬件和软件来监控有形资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

以模拟用户交互的方式测试系统，以检测潜在问题或监控性能。你可以使用 Amazon S CloudWatch ynthetics 来创建这些测试。

T

tags

键值对，用作组织资源的元数据。 AWS 标签可帮助您管理、识别、组织、搜索和筛选资源。有关更多信息，请参阅标记您的 AWS 资源。

目标变量

您在监督式 ML 中尝试预测的值。这也被称为结果变量。例如，在制造环境中，目标变量可能是产品缺陷。

任务列表

一种通过运行手册用于跟踪进度的工具。任务列表包含运行手册的概述和要完成的常规任务列表。对于每项常规任务，它包括预计所需时间、所有者和进度。

测试环境

参见环境。

训练

为您的 ML 模型提供学习数据。训练数据必须包含正确答案。学习算法在训练数据中查找将输入数据属性映射到目标（您希望预测的答案）的模式。然后输出捕获这些模式的 ML 模型。然后，您可以使用 ML 模型对不知道目标的新数据进行预测。

中转网关

中转网关是网络中转中心，您可用它来互连 VPC 和本地网络。有关更多信息，请参阅 AWS Transit Gateway 文档中的什么是公交网关。

基于中继的工作流程

一种方法，开发人员在功能分支中本地构建和测试功能，然后将这些更改合并到主分支中。然后，按顺序将主分支构建到开发、预生产和生产环境。

可信访问权限

向您指定的服务授予权限，该服务可以代表您在其账户中执行任务。 AWS Organizations 当需要服务相关的角色时，受信任的服务会在每个账户中创建一个角色，为您执行管理任务。有关更多信息，请参阅 AWS Organizations 文档中的AWS Organizations 与其他 AWS 服务一起使用。

优化

更改训练过程的各个方面，以提高 ML 模型的准确性。例如，您可以通过生成标签集、添加标签，并在不同的设置下多次重复这些步骤来优化模型，从而训练 ML 模型。

双披萨团队

一个小 DevOps 团队，你可以用两个披萨来喂食。双披萨团队的规模可确保在软件开发过程中充分协作。

U

不确定性

这一概念指的是不精确、不完整或未知的信息，这些信息可能会破坏预测式 ML 模型的可靠性。不确定性有两种类型：认知不确定性是由有限的、不完整的数据造成的，而偶然不确定性是由数据中固有的噪声和随机性导致的。有关更多信息，请参阅量化深度学习系统中的不确定性指南。

无差别任务

也称为繁重工作，即创建和运行应用程序所必需的工作，但不能为最终用户提供直接价值或竞争优势。无差别任务的示例包括采购、维护和容量规划。

上层环境

参见环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

两个 VPC 之间的连接，允许您使用私有 IP 地址路由流量。有关更多信息，请参阅 Amazon VPC 文档中的什么是 VPC 对等连接。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

一种包含经常访问的当前相关数据的缓冲区缓存。数据库实例可以从缓冲区缓存读取，这比从主内存或磁盘读取要快。

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

一个 SQL 函数，用于对一组以某种方式与当前记录相关的行进行计算。窗口函数对于处理任务很有用，例如计算移动平均线或根据当前行的相对位置访问行的值。

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

迁移项目中负责一组特定任务的职能小组。每个工作流都是独立的，但支持项目中的其他工作流。例如，组合工作流负责确定应用程序的优先级、波次规划和收集迁移元数据。组合工作流将这些资产交付给迁移工作流，然后迁移服务器和应用程序。

蠕虫

参见一次写入，多读。

WQF

请参阅 AWS 工作负载资格框架。

一次写入，多次读取 (WORM)

一种存储模型，它可以一次写入数据并防止数据被删除或修改。授权用户可以根据需要多次读取数据，但他们无法对其进行更改。这种数据存储基础架构被认为是不可变的。

Z

零日漏洞利用

一种利用未修补漏洞的攻击，通常是恶意软件。

零日漏洞

生产系统中不可避免的缺陷或漏洞。威胁主体可能利用这种类型的漏洞攻击系统。开发人员经常因攻击而意识到该漏洞。

僵尸应用程序

平均 CPU 和内存使用率低于 5% 的应用程序。在迁移项目中，通常会停用这些应用程序。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。