



Amazon RDS for MySQL 和 MariaDB 的监控和提醒工具及最佳实践

# AWS 规范性指导



# AWS 规范性指导: Amazon RDS for MySQL 和 MariaDB 的监控和提醒工具及最佳实践

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

# Table of Contents

简介 .....	1
概览 .....	2
目标业务成果 .....	2
一般最佳实践 .....	4
监控工具 .....	6
Amazon RDS 中包含的工具 .....	6
CloudWatch 命名空间 .....	7
CloudWatch 告警和控制面板 .....	8
Amazon RDS 性能详情 .....	9
增强监控 .....	11
其他 AWS 服务 .....	11
第三方监控工具 .....	12
Prometheus 和 Grafana .....	12
Percona .....	13
数据库实例监控 .....	15
数据库实例的性能详情指标 .....	15
数据库负载 .....	16
Dimensions .....	16
计数器指标 .....	17
SQL 统计数据 .....	19
CloudWatch 数据库实例的指标 .....	20
将 Performance Insights CloudWatch .....	20
操作系统监控 .....	22
事件、日志和审计跟踪记录 .....	29
Amazon RDS 事件 .....	29
数据库日志 .....	32
审核跟踪 .....	35
示例 .....	36
其他 CloudTrail 和 CloudWatch Logs 功能 .....	38
警报 .....	40
CloudWatch 警报 .....	40
EventBridge 规则 .....	43
指定操作、启用和禁用告警 .....	44
后续步骤和资源 .....	46

文档历史记录 .....	47
术语表 .....	48
# .....	48
A .....	48
B .....	51
C .....	52
D .....	55
E .....	58
F .....	60
G .....	61
H .....	62
我 .....	63
L .....	65
M .....	66
O .....	70
P .....	72
Q .....	74
R .....	75
S .....	77
T .....	80
U .....	81
V .....	82
W .....	82
Z .....	83
.....	lxxxiv

# Amazon RDS for MySQL 和 MariaDB 的监控和提醒工具及最佳实践

Igor Obradovic , Amazon Web Services ( AWS )

2025 年 3 月 ( [文档历史记录](#) )

数据库监控是衡量、跟踪和评测数据库可用性、性能和功能的过程。监控和提醒解决方案可帮助组织确保数据库服务以及关联的应用程序和工作负载安全、高性能、韧性和高效。开启后 AWS，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性能符合预期，并在任何问题影响客户之前对其进行检测和修复。您应使用所监控的指标、日志、事件和跟踪，以在超出阈值时发出告警。

本指南介绍 Amazon Relational Database Service ( Amazon RDS ) 数据库的可观测性和监控工具及最佳实践。该指南重点介绍了 MySQL 和 MariaDB 数据库，但其中大部分信息也适用于其他 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 DBAs、高级 DevOps 工程师和其他团队成员，他们为在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。AWS 云

## 内容

- [概述](#)
- [一般最佳实践](#)
- [监控工具](#)
- [数据库实例监控](#)
- [操作系统监控](#)
- [事件、日志和审计跟踪记录](#)
- [提示](#)
- [后续步骤和资源](#)

# 概览

监控和提醒包含在 [AWS Well-Architected 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。诸如 [Amazon Relational Database Service \( Amazon RDS \)](#) 之类的 AWS 服务提供必要的信息，以便您了解工作负载的内部状态（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 提供监控工具，可帮助您确定组织和业务成果何时处于危险之中或可能面临风险，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。在测量值超出预期边界时，您可以自动发出告警。我们建议您不仅要使用告警来发送通知，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**将监控和提醒定义为确保满足可用性要求至关重要。您的监控解决方案必须能够有效地检测故障。当检测到问题或故障时，其主要目标是对这些问题发出提醒。对于云中的韧性架构而言，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、横向扩展和容量预调配的设计原则取决于准确的监控和提醒服务。
- **安全支柱**讨论了对意外或不必要的配置更改及意外行为的检测和预防。您可以使用 [MariaDB 审计插件](#)配置 Amazon RDS for MySQL 和 MariaDB 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提醒工具中。系统会实时分析日志文件，以检测数据库中是否存在异常或可疑行为。此类意外或可疑行为可能表示您的 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，则会激活告警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

在监控和提醒机制中实施最佳实践可以帮助您确保为各种应用程序和工作负载提供高性能、韧性、高效、安全和成本优化的基础设施。您可以使用可观测性工具来实时收集、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整体情况，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，则监控和提醒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提醒解决方案可帮助您实现以下业务成果：

- **改善客户体验。**可靠的服务可改善您的客户体验。数据库通常是数字服务的关键组件，例如网络和移动应用程序、媒体流、支付、企业对企业 ( B2B ) API 和集成服务。如果您能够在数据库上监控和设置提醒以快速检测问题，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，从而为您的平台带来更多业务。例如，提供可靠在线服务的付款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，以及产生更多收入的新型创新服务。
- **避免经济损失。**数据库基础设施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。违反服务水平协议 ( SLA ) 可能会导致客户失去信任，从而导致收入损失。它也可以成为昂贵诉讼的法律依据，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 万到 54 万美元之间，具体取决于企业的类型和规模。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。**监控和提醒机制可以帮助您设计、开发和运营高可用性、韧性、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。您希望您的组织随着时间的推移而扩展并蓬勃发展，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。**高效的开发者如果在开发任务中没有遇到问题和瓶颈，就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，开发者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构件和基础设施组件，并有助于确定对最终用户的影响。合适的监控和提醒工具套件可以帮助开发者更好、更快地进行编码和测试。
- **提高运营效率和效益。**当您大规模运行云工作负载时，即使性能提升幅度很小，也能节省数百万美元。通过监控数据库并分析指标、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、修复问题及规划改进。

# 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，并针对操作事件和监控数据采取适当措施。

- 识别 KPI。根据预期的业务成果识别关键绩效指标 ( 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，那么您预期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。为了实现这一业务成果，您需要为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 设置为每周的 99.99%。根据基准值评估实际可用性 KPI 可以帮助您确定是否满足预期的数据库可用性 99.99%，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 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成果，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)
```

指标代表一个按时间顺序排列的数据点集。指标还可以包括维度，这对于分类和分析非常有用。

- 收集和分析工作负载指标。根据您的配置，Amazon RDS 会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 Amazon Elastic Compute Cloud ( Amazon EC2 ) 实例的总内存量。监测工具应对收集的指标进行定期、主动的分析，以识别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。为指标建立基准，以定义预期值并识别好坏阈值。例如，在正常的数据库操作下，您可以将 `ReadIOPS` 的基准定义为最多 1000。然后，您可以使用此基准进行比较，并确定是否存在过度使用的情况。如果您的新指标始终显示读取 IOPS 在 2000-3000 范围内，则表明您已经发现了一个可能触发调查、干预和改进响应的偏差。
- 当工作负载结果面临风险时发出提醒。当您确定业务成果面临风险时，发出提醒。然后，您既可以在问题影响客户之前主动解决问题，也可以及时缓解事件的影响。
- 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 提供了[监控工具](#)，这些工具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提醒。在 Amazon RDS 工作负载的操作中检测到异常时，请发出提醒，以便在必要时采取适当措施进行响应。

- 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，并确定为实现业务目标而可能改进的领域。验证衡量指标和评估的关键绩效指标的有效性，并在必要时对其进行修改。例如，假设您为并发数据库连接的最佳数量设置了 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。您的数据库连接数可能超过了 KPI 基准定义的连接数。通过分析您当前指标，您可以检测结果，但可能无法确定根本原因。如果出现这种情况，您应该修改指标并添加额外的监控措施，例如表锁定计数器。新的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测性、监控和提醒工具来执行以下操作：

- 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 实例做出明智的决策
- 分析指标和日志以主动预测潜在问题
- 在超出阈值时生成提醒，以便在用户受到影响之前排查并解决问题

您可以选择不同的选项和解决方案，包括 AWS 提供的云原生可观测性及监控工具和服务；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

- [Amazon RDS 中包含的工具](#)
- [CloudWatch 命名空间](#)
- [CloudWatch 告警和控制面板](#)
- [Amazon RDS 性能详情](#)
- [增强监控](#)
- [其他 AWS 服务](#)
- [第三方监控工具](#)

## Amazon RDS 中包含的工具

Amazon Relational Database Service ( Amazon RDS ) 是 AWS 云中的托管式数据库服务。由于 Amazon RDS 是一项托管服务，因此您无需处理大多数管理任务，例如数据库备份、操作系统 ( OS ) 和数据库软件安装、操作系统和软件补丁、高可用性设置、硬件生命周期及数据中心运营。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[可观测性](#)解决方案。

一些监控工具已包含在 Amazon RDS 服务中，且已预配置并自动启用。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、性能数据和配置而提供的，旨在提供指引。例如，引擎版本已过时建议表明您的数据库实例没有运行最新版本的数据库软件，您应该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 Amazon RDS 文档中的[查看 Amazon RDS 建议](#)。

## CloudWatch 命名空间

Amazon RDS 与 [Amazon CloudWatch](#) 集成，后者是一项针对 AWS 上运行的云资源和应用程序的监控和提醒服务。Amazon RDS 会自动收集有关数据库实例的操作、利用率、性能及运行状况的指标、日志文件、跟踪和事件，并将它们发送到 CloudWatch 进行长期存储、分析和提醒。

Amazon RDS for MySQL 和 Amazon RDS for MariaDB 每隔一分钟自动向 CloudWatch 发布一组默认指标，无需额外付费。这些指标收集到两个命名空间中，这两个命名空间是指标的容器：

- [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/使用情况命名空间](#) 包括账户级别的使用量指标，这些指标用于确定您是否在 [Amazon 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 将保留指标数据，如下所示：

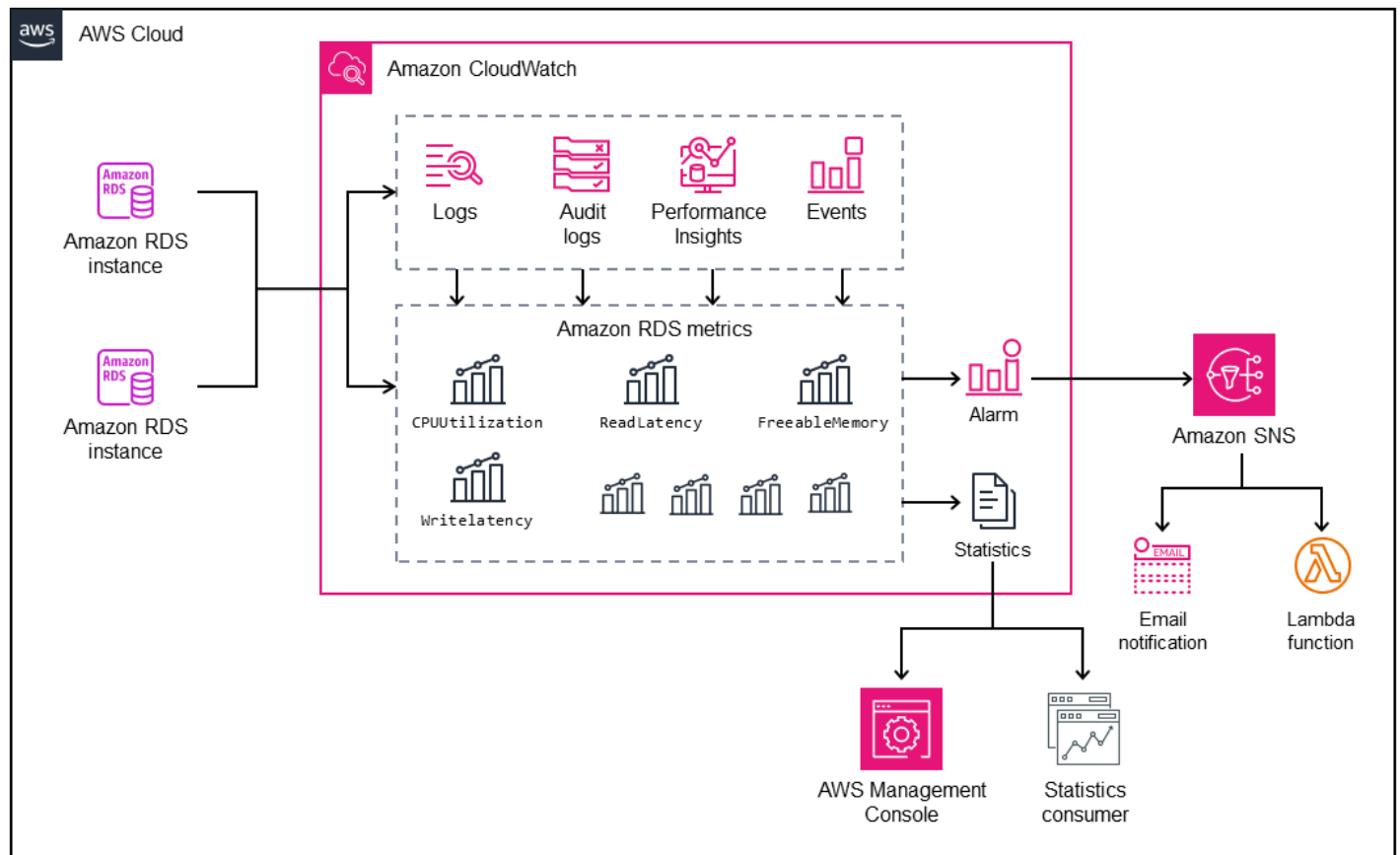
- 3 小时：周期小于 60 秒的高分辨率自定义指标将保留 3 小时。3 小时后，数据点将汇总为 1 分钟周期指标并保存 15 天。
- 15 天：周期为 60 秒 ( 1 分钟 ) 的数据点保留 15 天。15 天后，数据点将汇总为 5 分钟周期指标并保存 63 天。

- 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 3600 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](#)。

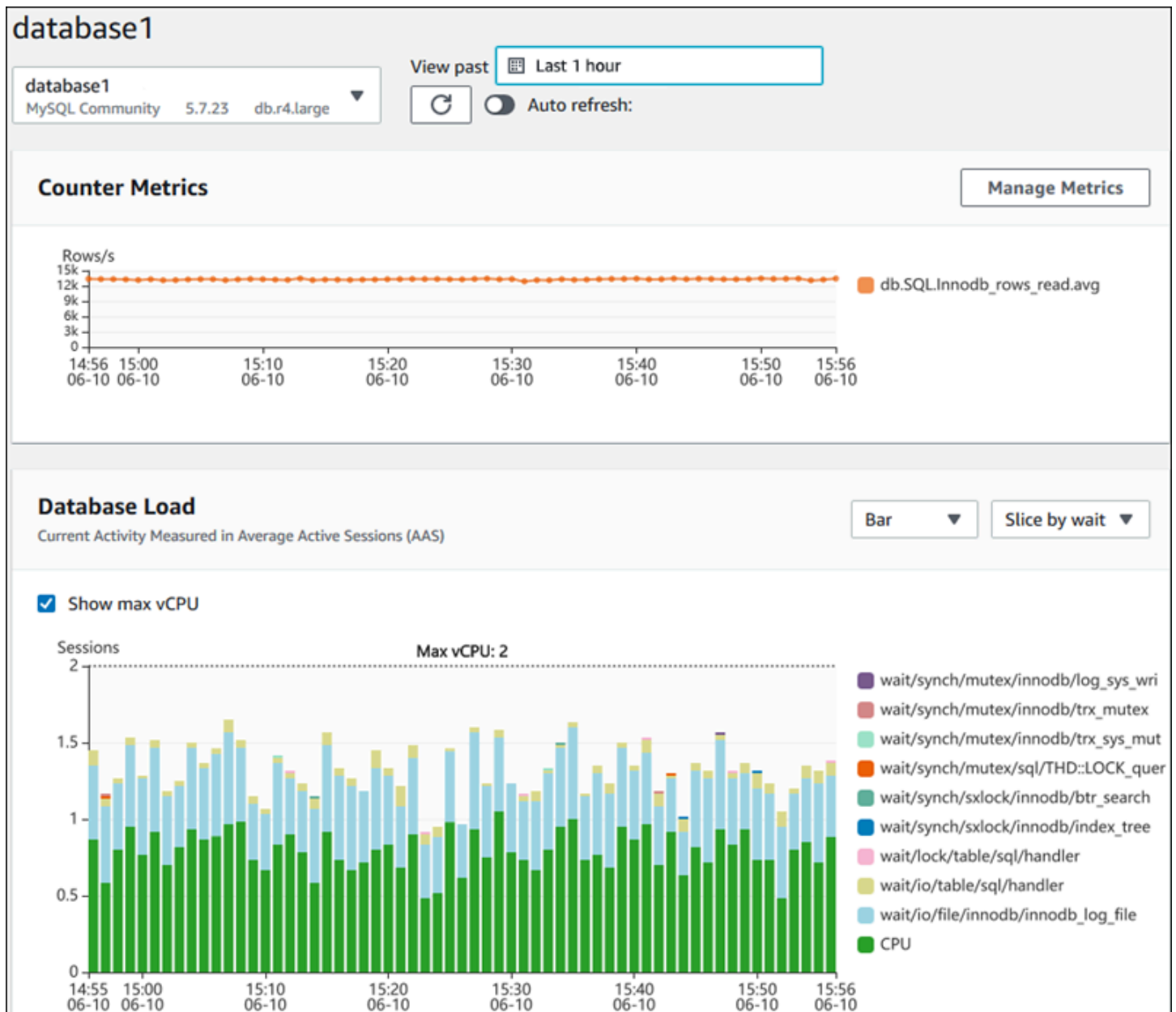
## CloudWatch 告警和控制面板

您可以使用 [Amazon CloudWatch 告警](#) 在特定时间段内监控特定 Amazon RDS 指标。例如，您可以监控 FreeStorageSpace，然后在指标值超出您设置的阈值时执行一个或多个操作。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），则告警将被激活，且可能触发一项操作，自动为 Amazon RDS 数据库实例预调配额外存储空间。告警还可以使用 Amazon Simple Notification Service（Amazon SNS）向 DBA 发送通知短信。下图阐明了此过程。



CloudWatch 还提供[控制面板](#)，您可以使用控制面板创建指标、自定义指标、与指标交互及保存指标的自定义视图（图表）。您还可以使用 [CloudWatch Logs Insights](#) 创建控制面板，用于监控慢速查询日





您必须在数据库实例创建过程中[启用性能详情](#)，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 100 万个 API 请求。（可选）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](#)。

有关如何使用性能详情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。

性能详情会[自动将指标发布到 CloudWatch](#)。除了使用性能详情工具外，您还可以利用 CloudWatch 提供的其他功能。您可以使用 CloudWatch 控制台、AWS CLI 或 CloudWatch API 来检查性能详情指标。您还可以像添加任何其他指标一样添加 CloudWatch 告警。例如，如果 DBLoad 指标超出您设置

的阈值，您可能希望触发向 DBA 的 SMS 通知或采取纠正措施。您还可以将性能详情指标添加到现有的 CloudWatch 控制面板。

## 增强监控

[增强监控](#)是一个可以实时捕获 Amazon RDS 数据库实例运行所在操作系统 ( OS ) 的指标的工具。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。与性能详情一样，增强监控指标从 Amazon RDS 传输到 CloudWatch，您可以从其他功能中受益，例如长期保存指标以供分析、创建指标筛选条件、在 CloudWatch 控制面板上显示图表以及设置告警。默认情况下，在创建新的 Amazon RDS 数据库实例时禁用增强监控。在创建或修改数据库实例时，可以[启用](#)此功能。定价基于从 Amazon RDS 传输到 CloudWatch Logs 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 Logs 免费套餐内。有关完整的定价详细信息，请参阅 [Amazon CloudWatch 定价](#)。有关此工具的更多信息，请参阅 [Amazon RDS 文档](#) 和 [增强监控](#) 常见问题。

## 其他 AWS 服务

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

- [Amazon EventBridge](#) 是一种无服务器事件总线，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。Amazon RDS 事件表示 Amazon RDS 环境中的更改。例如，当数据库实例将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 将事件近乎实时地传输到 CloudWatch Events 和 EventBridge。使用 EventBridge 和 CloudWatch Events，您可以定义规则，以针对感兴趣的特定 Amazon RDS 事件发送提醒，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，例如可以执行纠正措施的 AWS Lambda 函数，或者可以发送邮件或 SMS 通知 DBA 或 DevOps 工程师有关事件的 Amazon SNS 主题。
- [Amazon CloudWatch Logs](#) 是一项集中存储所有应用程序、系统和 AWS 服务 ( 包括 Amazon RDS for MySQL 和 MariaDB 数据库实例及 AWS CloudTrail ) 中的日志文件的服务。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 Logs：
  - 错误日志
  - 慢速查询日志
  - 常规日志
  - 审核日志

您可以使用 CloudWatch Logs Insights 查询和分析日志数据。该功能包括一种专用查询语言，可帮助您搜索与您定义的模式匹配的日志事件。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控制面板，或者在超出定义的阈值时设置告警。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、发送提醒并采取纠正措施。您可以使用 AWS 管理控制台、AWS CLI、Amazon RDS API 或适用于 CloudWatch Logs 的 AWS SDK，来访问和管理数据库日志。

- [AWS CloudTrail](#) 会记录并持续监控 AWS 账户中的用户和 API 活动。它可以帮助您对 Amazon RDS for MySQL 或 MariaDB 数据库实例进行审计、安全监控和运营问题排查。CloudTrail 与 Amazon RDS 集成。所有操作都可以记录，CloudTrail 提供 Amazon RDS 中用户、角色或 AWS 服务执行的操作记录。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，且日志包括有关所请求的操作 ("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"}) 等方面的信息。CloudTrail 记录的事件包括来自 Amazon 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 AWS 为 Amazon RDS 提供的全套云原生可观测性和监控工具之外，您可能还需要使用其他软件供应商的监控工具。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 AWS 云中运行。如果您已建立企业可观测性解决方案，则可能需要继续使用现有工具并将其扩展到您的 AWS 云部署中。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，您可以在 CloudWatch 和其他 AWS 云服务之上进行构建，将许多第三方监控解决方案与 Amazon RDS 集成。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、可视化和提醒。其中一些第三方解决方案包括 Prometheus、Grafana 和 Percona。

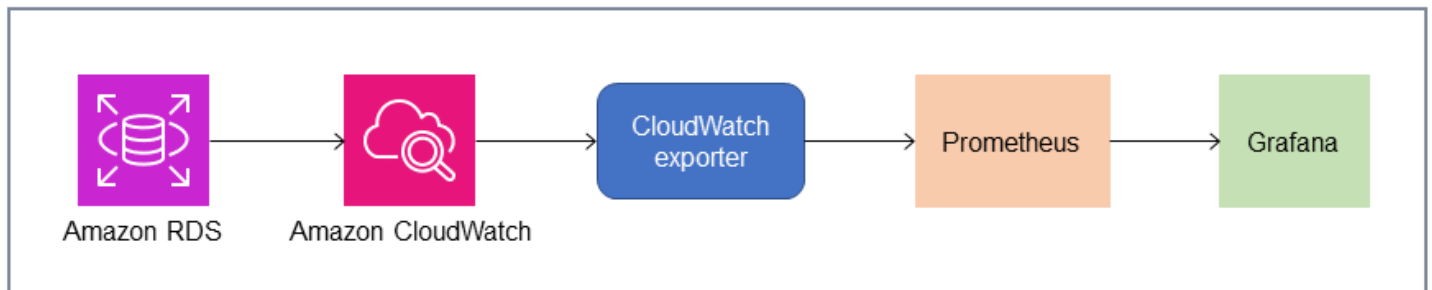
## Prometheus 和 Grafana

[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，使用开源导出程序（例如 YACE 导出程序或 CloudWatch 导出程序）将指标导出到 Prometheus 服务器。

- [YACE 导出程序](#)通过在 CloudWatch API 的单个请求中检索多个指标，从而优化数据导出任务。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提醒。
- [CloudWatch 导出程序](#)由 Prometheus 官方维护。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。

在选择导出程序、设计部署模型及配置导出程序实例时，考虑 [CloudWatch](#) 和 [CloudWatch Logs](#) 服务及 API 配额，因为将 CloudWatch 指标导出到 Prometheus 服务器是基于 CloudWatch API 实现的。例如，在单个 AWS 账户和区域中部署多个 CloudWatch 导出程序实例来监控数百个 Amazon RDS 数据库实例，可能会导致节流错误 (ThrottlingException) 和代码 400 错误。要克服此类限制，请考虑使用 YACE 导出程序，该导出程序经过优化，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 AWS 账户，并限制每个 AWS 账户中的导出程序实例数量。

提醒由 Prometheus 服务器生成并由 [Alertmanager](#) 处理。此工具负责对提醒进行重复数据删除、分组和路由到正确的接收者，例如邮件、SMS 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 提供丰富的可视化小组件，例如高级图表、动态控制面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，并包括提醒功能，以持续评估指标和日志，并在数据与提醒规则匹配时发送通知。



## Percona

[Percona 监控和管理 \(PMM\)](#) 是一款免费的[开源](#)数据库监控、管理和可观测性解决方案，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。它提供了用于在控制面板中可视化数据的 Web 用户界面以及其他功能，例如用于数据库运行状况评测的自动顾问。您可以使用 PMM 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，查询服务器统计数据、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 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。PMM 工具专为数据库监控而设计，且比

Prometheus 收集更多数据库特定指标。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，它直接从 MySQL 和 MariaDB 数据库实例中查询 `performance_schema`，以获取指标。PMM 的突出特点之一是它能够就该工具在数据库中发现的问题向 DBA [发出提醒](#)和建议。PMM 提供一系列检查，可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 集成的商业可观测性和监控解决方案。示例包括 [Datadog 数据库监控](#)、[Dynatrace Amazon RDS 监控](#)和 [AppDynamics 数据库监控](#)。

# 数据库实例监控

[数据库实例](#)是 Amazon RDS 的基本构建块。它是在云中运行的独立数据库环境。对于 MySQL 和 MariaDB 数据库，数据库实例是 my [sqld](#) 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、thread/connection 处理程序、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专门的使用案例。默认且推荐使用的存储引擎是 [InnoDB](#)，它是一个事务性的通用型关系数据库引擎，符合原子性、一致性、隔离性、持久性 (ACID) 模型。InnoDB 具有[内存结构](#) (缓冲池、更改缓冲区、自适应哈希索引、日志缓冲区) 以及[磁盘结构](#) (表空间、表、索引、撤消日志、重做日志、双写缓冲区文件)。为了确保您的数据库严格遵循 ACID 模型，[InnoDB 存储引擎实施了许多功能](#)来保护您的数据，包括事务、提交、回滚、崩溃恢复、行级别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、完整性和安全性维持在预期且令人满意的性能水平。根据您的工作负载，每个组件和功能都可能对 CPU、内存、网络 and 存储子系统带来相应的资源需求。对特定资源的需求激增超过该资源的预调配容量或软件限制 (由配置参数或软件设计决定) 时，数据库实例可能会出现性能下降或完全不可用和损坏的情况。因此，必须测量和监控这些内部组件，将其与定义的基准值进行比较，并在监控值偏离预期值时生成提醒。

如前所述，您可以使用不同的[工具](#)来监控 MySQL 和 MariaDB 实例。我们建议您使用 Amazon RDS Performance Insight CloudWatch s 和工具进行监控和警报，因为这些工具已与 Amazon RDS 集成，可以收集高分辨率指标，近乎实时地呈现最新的性能信息，并生成警报。

无论您首选哪种监控工具，我们都建议您在 MySQL 和 MariaDB 数据库实例中[开启性能架构](#)。[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) 的运行，旨在最大限度地减轻对数据库整体性能的影响。您可以使用 performance\_schema 参数管理此功能。虽然此参数是可选的，但您必须使用它来收集高分辨率 (每秒一次) 的每个 SQL 指标、活跃会话指标、等待事件和其他详细的低级别监控信息，这些信息由 Amazon RDS 性能详情收集。

## Sections

- [数据库实例的性能详情指标](#)
- [CloudWatch 数据库实例的指标](#)
- [将 Performance Insights CloudWatch](#)

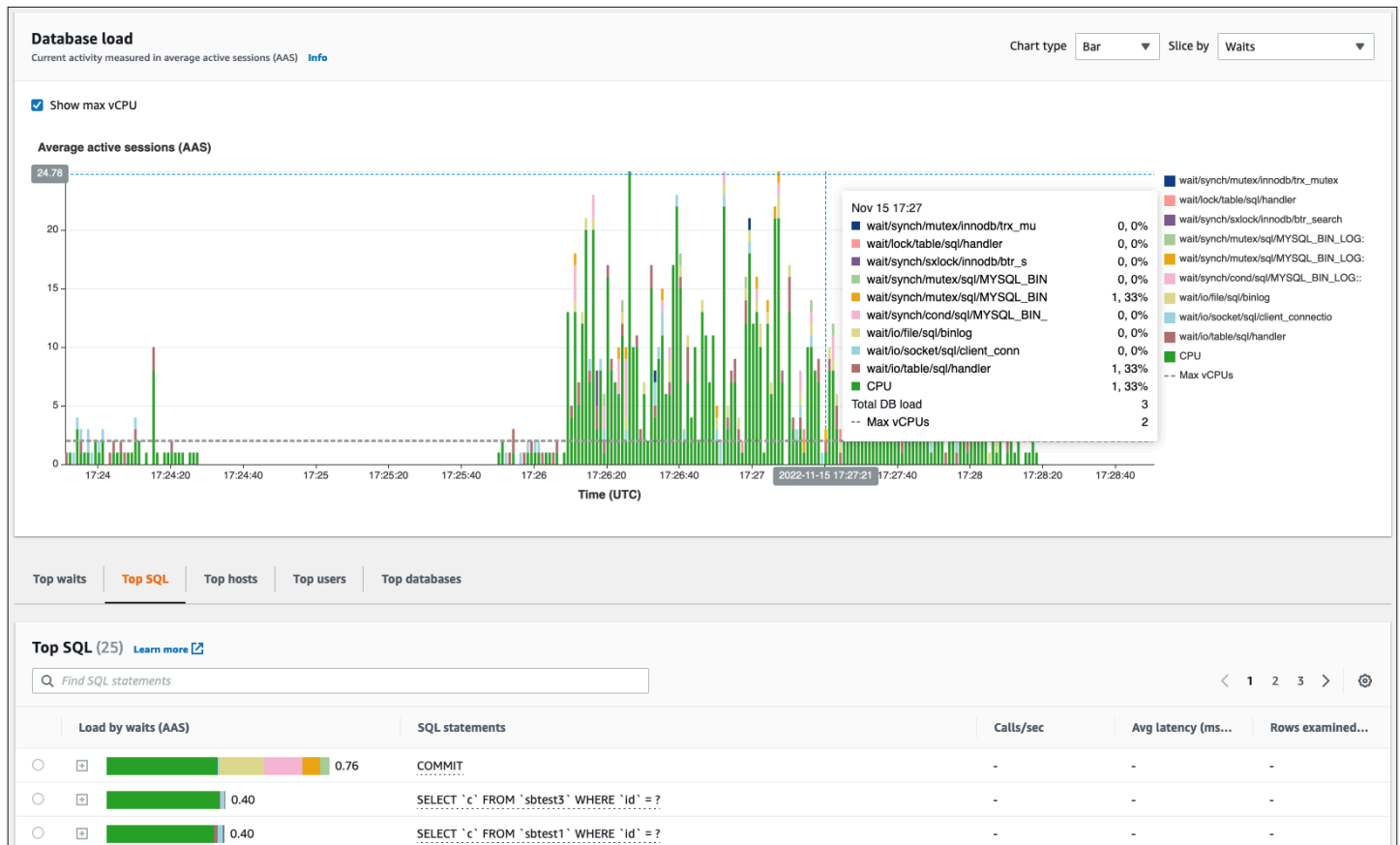
## 数据库实例的性能详情指标

性能详情会监控不同类型的指标，如以下各部分所述。

## 数据库负载

数据库负载 ( DBLoad ) 是性能详情中的一项关键指标，用于衡量数据库中的活动水平。它每秒收集一次，并自动发布到 Amazon CloudWatch。它以平均活跃会话数 ( AAS ) 表示数据库实例的活动，即同时运行 SQL 查询的会话数。DBLoad 指标与其他时间序列指标不同，因为它可以使用以下五个维度中的任何一个来解释：等待、SQL、主机、用户和数据库。这些维度是 DBLoad 指标的子类别。您可以将其用作切片依据类别，以表示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说明，请参阅 Amazon RDS 文档中的[数据库负载](#)。

以下屏幕插图显示了性能详情工具。



## Dimensions

- 等待事件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。如果您运行诸如 `SELECT * FROM big_table` 和之类的 SQL 语句，如果此表比分配的 InnoDB 缓冲池大得多，则您的会话很可能会 `wait/io/file/innodb/innodb_data_file` 等待等待事件，这些事件是由对数据文件的物理 I/O 操作引起的。等待事件是数据库监控的一个重要维度，因为它们可以指示可能的性能瓶颈。等待事件指示您在会话内运行的 SQL 语句等待时间最长的资源和操作。例如，当数据库活动频繁且事务数量庞大时，会发生 `wait/synch/mutex/innodb/trx_sys_mutex` 事件；

当线程获取 InnoDB 缓冲池的锁以访问内存中的页面时，会发生 `wait/synch/mutex/innodb/buf_pool_mutex` 事件。有关所有 MySQL 和 MariaDB 等待事件的信息，请参阅 MySQL 文档中的 [Wait Event Summary Tables](#)。要了解如何解释工具名称，请参阅 MySQL 文档中的 [Performance Schema Instrument Naming Conventions](#)。

- SQL 显示哪些 SQL 语句对数据库总负载贡献最大。位于 Amazon RDS 性能详情中数据库负载图表下方的主要维度表是交互式的。通过单击按等待状态排列的负载 ( AAS ) 列中的栏，您可以获取与 SQL 语句关联的等待事件的详细列表。当您在列表中选择 SQL 语句时，性能详情会在数据库负载图表中显示关联的等待事件，在 SQL 文本部分中显示相应的 SQL 语句文本。SQL 统计信息显示在主要维度表的右侧。
- 主机显示所连接客户端的主机名 此维度可帮助您确定哪些客户端主机正在向数据库发送大部分负载。
- 用户按登录数据库的用户对数据库负载进行分组。
- 数据库按客户端所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之前的值。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 ( 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 引擎无法从缓冲池中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。

有关所有原生指标的定义，请参阅 MySQL 文档中的[服务器状态变量](#)。

- [非原生计数器](#)由 Amazon RDS 定义。您可以使用特定的查询来获取这些指标，也可以通过在计算中使用两个或多个原生指标来推导这些指标。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 在不利用磁盘的情况下可以从缓冲池中检索的读取操作数。它是根据原生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
```

- `I0.innoDB_datafile_writes_to_disk` 表示 InnoDB 数据文件向磁盘写入操作的次数。它只捕获对数据文件的操作，而不是双重写入或重做日志记录写入操作。按如下方式计算：

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

您可以在性能详情控制面板中直接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。

### Select metrics shown on the graph ✕

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

▼ SQL

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

▼ Locks

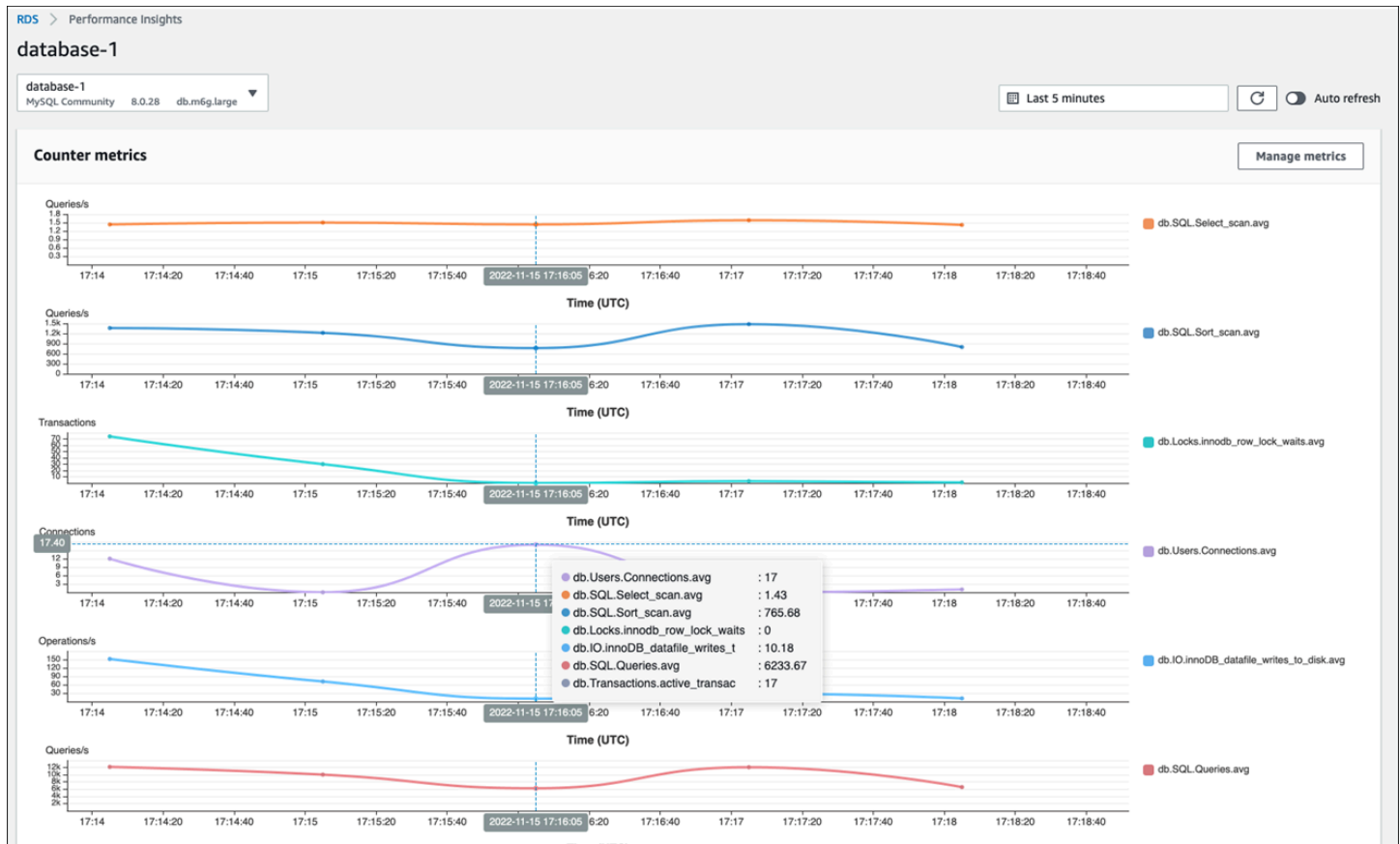
<input type="checkbox"/> Innodb_row_lock_time	<input checked="" type="checkbox"/> innodb_row_lock_waits
<input type="checkbox"/> innodb_deadlocks	<input type="checkbox"/> innodb_lock_timeouts
<input type="checkbox"/> Table_locks_immediate	<input type="checkbox"/> Table_locks_waited

▼ Users

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

Cancel
Update graph

选择更新图表按钮，以显示您选择的指标，如下图所示。



## SQL 统计数据

性能详情会收集与 SQL 查询相关的性能指标，包括查询运行的每一秒以及每次 SQL 调用。通常，性能详情会在语句和摘要级别收集 [SQL 统计数据](#)。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本值的查询的复合指标。摘要用变量替换特定的文本值；例如：

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

- 有些指标表示每秒处理的每个已解析 SQL 语句的统计数据。例如，`sql_tokenized.stats.count_star_per_sec` 表示每秒调用次数（即 SQL 语句每秒运行的次数）。
- 性能详情还包括提供 SQL 语句每次调用统计数据的指标。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 统计数据可在“性能详情”控制面板的主要维度表中的主要 SQL 选项卡中找到。

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

## CloudWatch 数据库实例的指标

亚马逊 CloudWatch 还包含亚马逊 RDS 自动发布的指标。位于 AWS/RDS 命名空间中的指标是实例级指标，指的是 Amazon RDS ( 服务 ) 实例 ( 即在云中运行的独立数据库环境 ) ，而不是严格意义上的 [mysqld](#) 流程中的数据库实例。因此，按照该术语的严格定义，这些[默认指标](#)中的大多数都属于操作系统指标的类别。示例包括：CPUUtilization、WriteIOPS、SwapUsage 及其他。不过，有一些适用于 MariaDB 和 MySQL 的数据库实例指标：

- BinLogDiskUsage：二进制日志所占的磁盘空间大小。
- DatabaseConnections：连接至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量。

## 将 Performance Insights CloudWatch

Amazon RDS Performance Insights 监控大部分数据库实例指标和维度，并通过 AWS 管理控制台上的 Performance [Insights 控制面板提供这些指标](#)和维度。此控制面板非常适合数据库问题排查和根本原因分析。但是，无法在性能详情中为与性能相关的指标创建告警。如果要基于 Performance Insights 指标创建警报，则这些指标必须包含在中 CloudWatch。

Performan [ce Insights 自动向发布指标 CloudWatch](#)。您可以从 Performance Insights 中 CloudWatch 查询相同的数据，但是将指标包含在中可以轻松添加 CloudWatch 警报并将指标添加到现有 CloudWatch 仪表板中。[计数器](#)是操作系统和数据库性能指标，例如 os.memory.free 或 db.Locks.InnoDB\_row\_lock\_time。操作系统指标收集取决于“增强监控”设置。如果关闭“增强监控”，则每分钟收集一次操作系统指标。如果开启“增强监控”，则会收集所选时间段内的操作系统指标。有关更多信息，请参阅 Amazon RDS 文档中的[开启和关闭“增强监控”](#)。

Performance Insights 允许您将数据库实例的[预配置或自定义指标控制面板](#)导出到 CloudWatch。您可以将指标仪表板导出为新的仪表板，也可以将其添加到现有 CloudWatch 仪表板中。将 Performance Insights 指标 CloudWatch 控制面板导出到控制面板，可以概述与系统中各种资源相关的指标，例如 EC2 实例、亚马逊弹性文件系统 (Amazon EFS) 资源和弹性负载均衡 (ELB) 资源，以及数据库实例指标，从而统一、全面地了解系统的运行状况。

您可以使用 CloudWatch DB\_PERF\_INSIGHTS 指标数学函数根据来自的 Performance Insights 指标查询和创建警报和图表 CloudWatch。要在 Performance Insights 指标上创建警报，请按照[CloudWatch 文档](#)中的说明进行操作。例如，如果您想在数据库实例中的活跃事务总数达到特定阈值时触发告警，请按照该页面上的说明进行操作，使用以下 DB\_PERF\_INSIGHTS 数学表达式，然后选择应用：

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

其中 db-BQ2TPYY7HG2GDFC7APMB3BVB3M 是数据库实例的资源 ID。指定时段（例如，1 分钟）和条件（例如，大于 1000）。要完成告警的创建，请配置告警操作，添加名称和描述，然后预览和创建告警。

## 操作系统监控

Amazon RDS for MySQL 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 and 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 被过度利用（即，如果负载需要的 CPU 处理能力超过为数据库实例预调配的 CPU 处理能力），则此问题将影响数据库的性能和稳定性，从而影响您的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，系统会将内存页面写入位于磁盘上的交换内存。由于磁盘比内存慢得多，因此即使磁盘基于 SSD NVMe 技术，内存分配过多也会导致性能下降。高内存利用率会导致数据库响应延迟增加，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至耗尽了 RAM 和交换内存空间，则数据库服务可能会变得不可用，用户可能会观察到诸如 [ERROR] mysqld: Out of memory (Needed xyz bytes) 之类的错误。

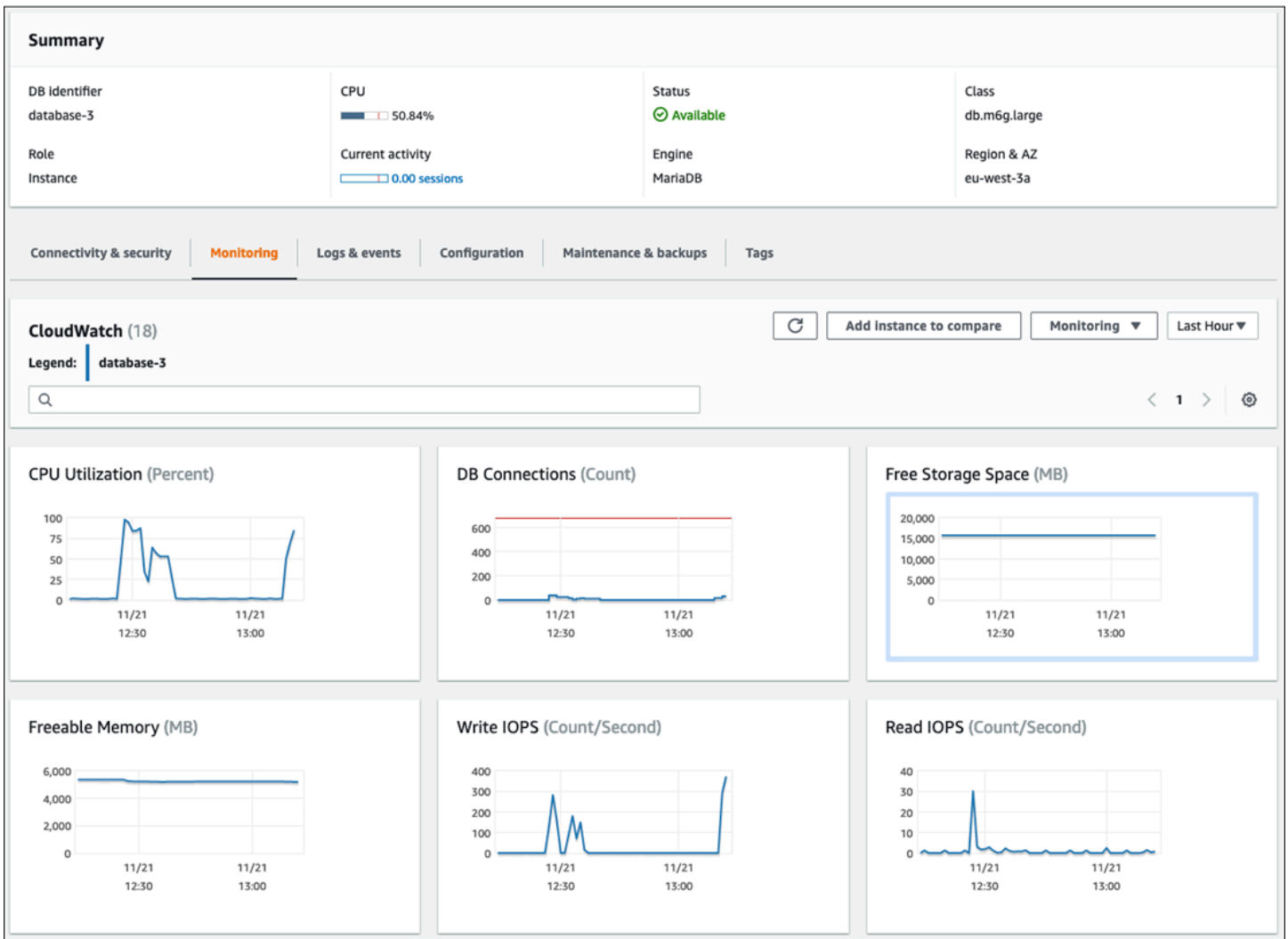
MySQL 和 MariaDB 数据库管理系统利用存储子系统，该子系统由磁盘组成，用于存储[磁盘上的结构](#)，例如表、索引、二进制日志、重做日志、撤消日志和双写缓冲区文件。因此，与其他类型的软件相比，数据库必须执行大量磁盘活动。为了确保数据库的最佳运行，监控和调整磁盘 I/O 利用率和磁盘空间分配非常重要。数据库达到磁盘支持的最大 IOPS 或吞吐量的限制时，数据库性能可能会受到影响。例如，索引扫描导致的随机访问爆发可能会导致每秒大量 I/O 操作，这最终可能会达到底层存储的限制。全表扫描可能未达到 IOPS 限制，但它们可能会导致以每秒兆字节为单位的高吞吐量。监控磁盘空间分配并生成提醒至关重要，因为诸如 OS error code 28: No space left on device 之类的错误可能会导致数据库不可用和损坏。

Amazon RDS 为数据库实例运行的操作系统实时提供指标。Amazon RDS 会自动向 CloudWatch 发布一组操作系统指标。您可以在 Amazon RDS 控制台和 CloudWatch 控制面板中显示和分析这些指标，且可以在 CloudWatch 中对所选指标设置告警。示例包括：

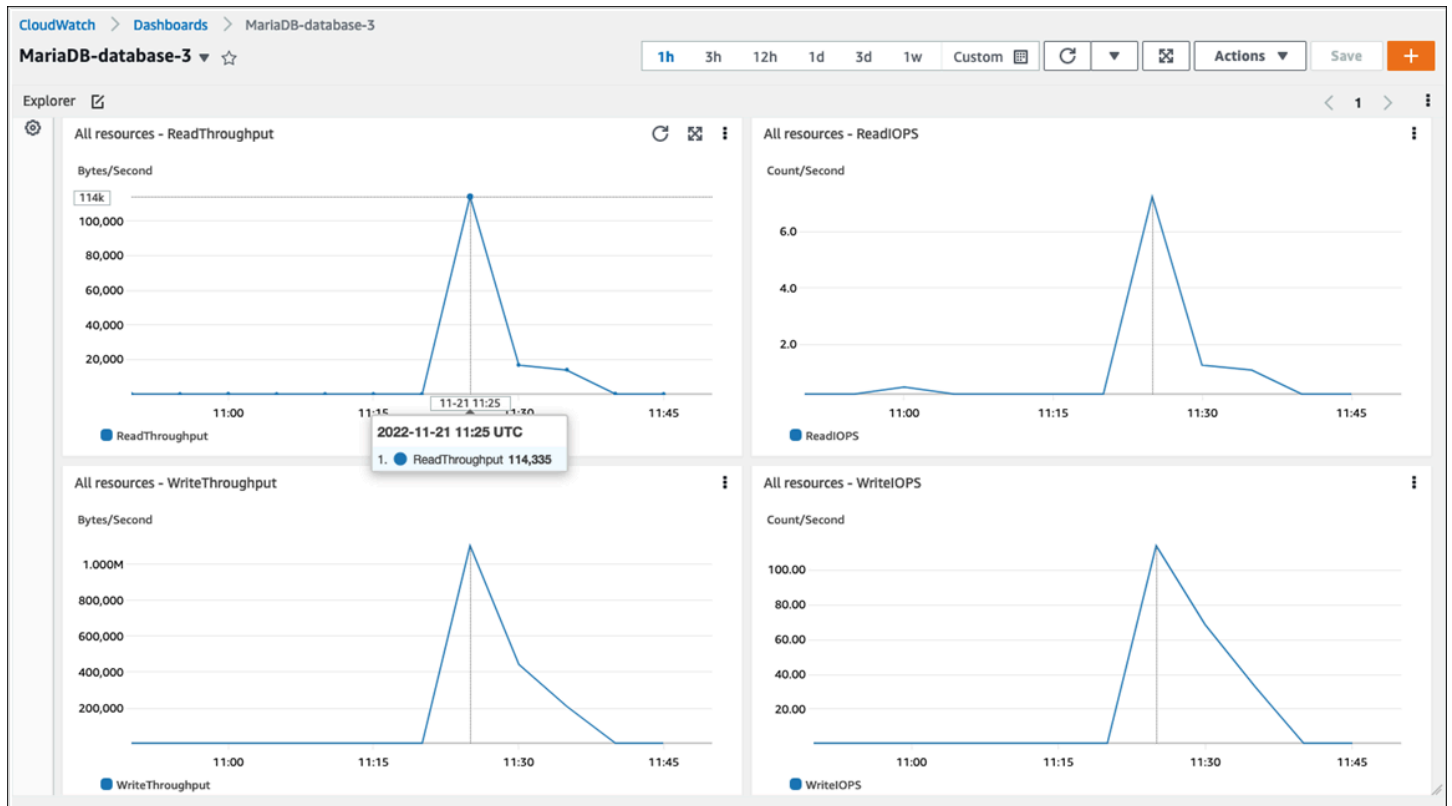
- CPUUtilization：CPU 使用百分率。
- BinLogDiskUsage：二进制日志所占的磁盘空间大小。
- FreeableMemory：随机存取内存的可用大小。这表示 /proc/meminfo 的 MemAvailable 字段的值。
- ReadIOPS：每秒平均磁盘读取 I/O 操作数。
- WriteThroughput：本地存储每秒写入磁盘的平均字节数。
- NetworkTransmitThroughput：数据库节点上的传出网络流量，它结合了数据库流量和用于监控和复制的 Amazon RDS 流量。

有关 Amazon RDS 向 CloudWatch 发布的所有指标的完整参考，请参阅 Amazon RDS 文档中的 [Amazon RDS 的 Amazon CloudWatch 指标](#)。

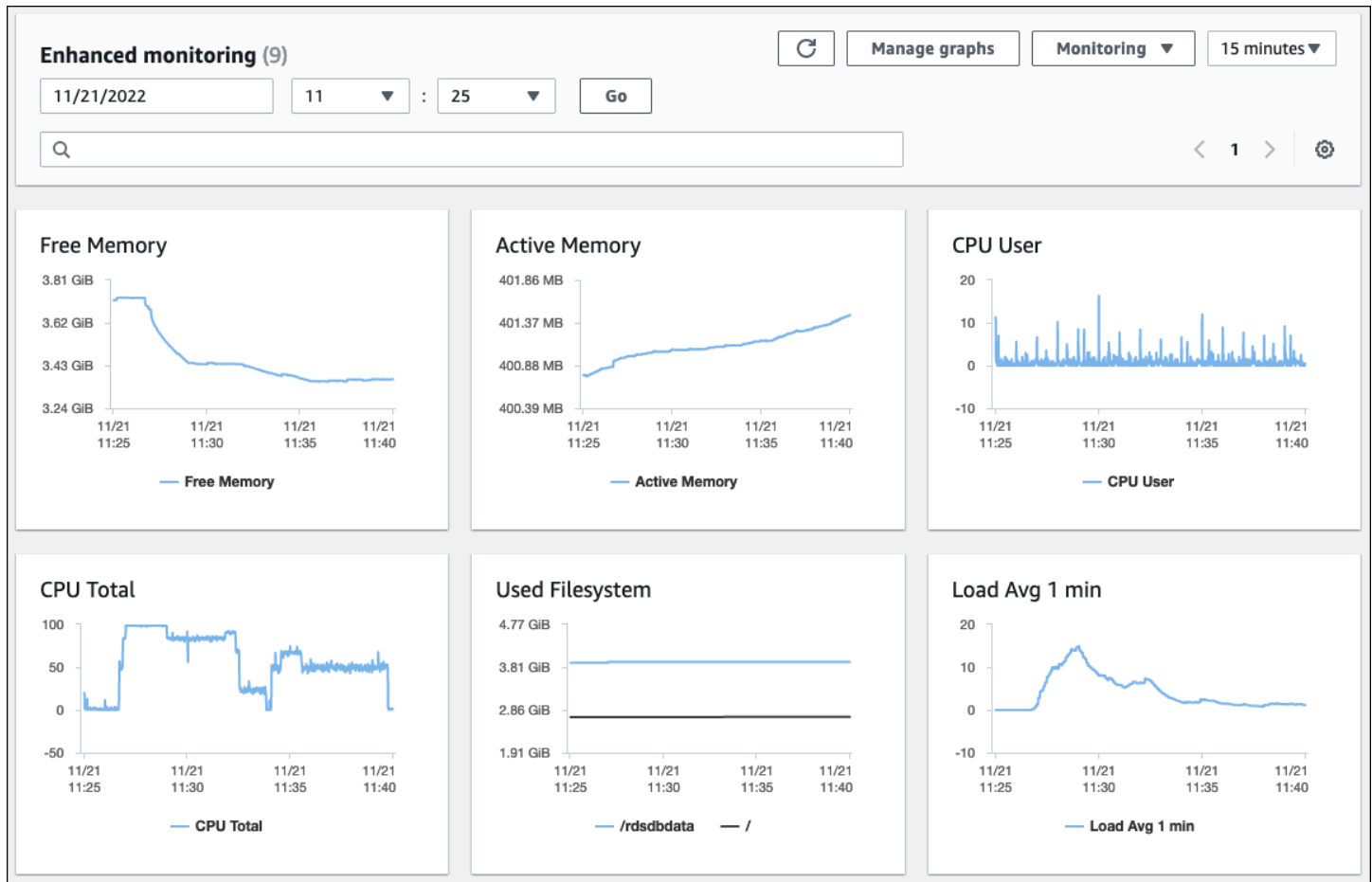
下图显示了 Amazon RDS 控制台上显示的 Amazon RDS 的 CloudWatch 指标示例。



下图显示了 CloudWatch 控制面板中显示的类似指标。



另一组操作系统指标由 Amazon RDS 的[增强监控](#)收集。该工具通过提供实时系统指标和操作系统进程信息，让您可以更深入了解 Amazon RDS for MariaDB 和 Amazon RDS for MySQL 数据库实例的运行状况。当您在数据库实例上[启用“增强监控”](#)并设置所需的粒度时，该工具会收集操作系统指标和进程信息，您可以在 [Amazon RDS 控制台](#)上显示和分析这些指标和流程信息，如以下屏幕所示。



“增强监控”提供的一些关键指标是：

- `cpuUtilization.total`：使用的 CPU 总百分比。
- `cpuUtilization.user`：用户程序使用的 CPU 百分比。
- `memory.active`：已分配的内存量（以 KB 为单位）。
- `memory.cached`：用于缓存基于文件系统的 I/O 的内存量。
- `loadAverageMinute.one`：过去 1 分钟内请求 CPU 时间的进程数。

有关指标的完整列表，请参阅 Amazon RDS 文档中的[“增强监控”中的操作系统指标](#)。

在 Amazon RDS 控制台上，操作系统进程列表提供了数据库实例中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**：本节汇总了所有内核和系统进程的摘要。这些进程通常对数据库性能的影响降至最低。

- RDS 进程：本节概述了支持 Amazon RDS 数据库实例所需的 AWS 进程。例如，其中包括 Amazon RDS 管理代理、监控和诊断进程以及类似的进程。
- RDS 子进程：本节概述了支持数据库实例的 Amazon RDS 进程，在本例中为 `mysqld` 进程及其线程。`mysqld` 线程似乎嵌套在父 `mysqld` 进程下。

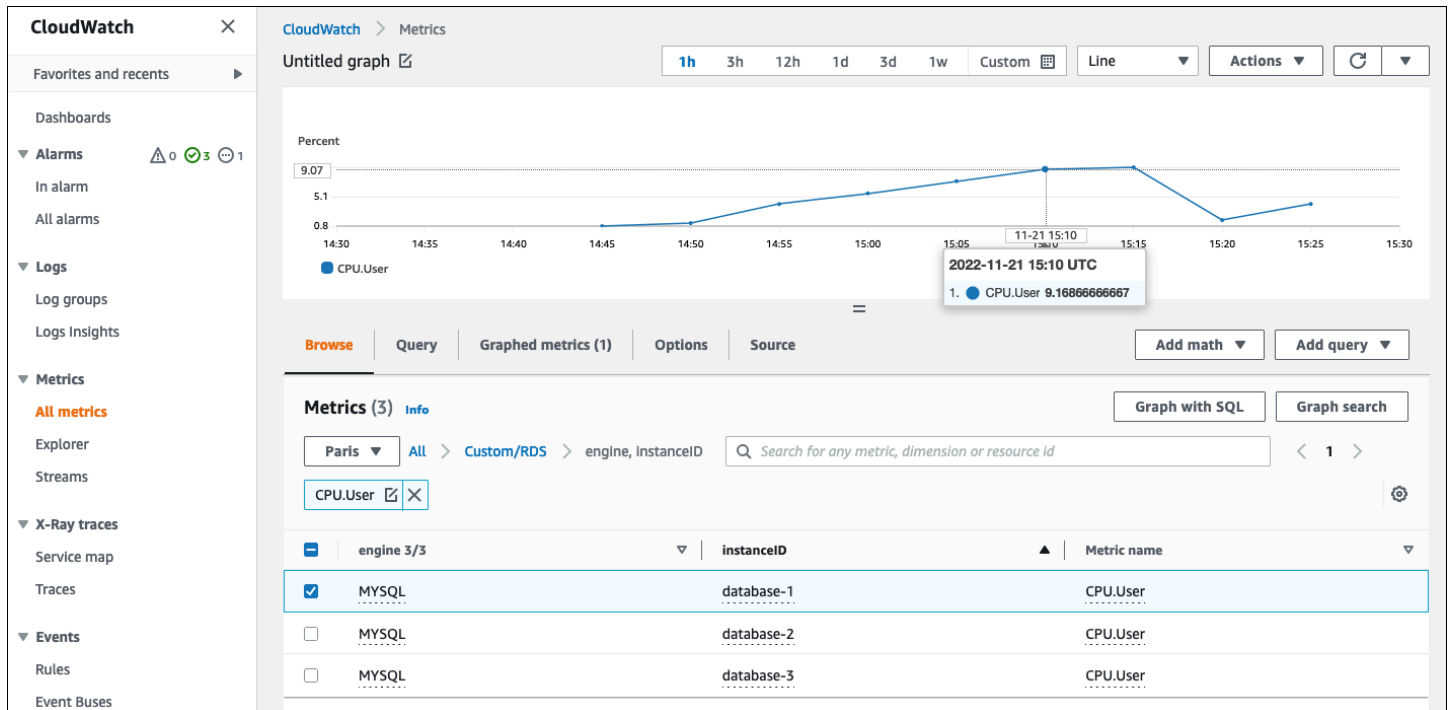
以下屏幕插图显示了 Amazon RDS 控制台中的操作系统进程列表。

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

Amazon RDS 将增强监测中的指标传输到您的 CloudWatch Logs 账户。Amazon RDS 控制台中显示的监控数据是从 CloudWatch Logs 中检索的。您还可以从 CloudWatch Logs 中[检索数据库实例的指标作为日志流](#)。这些指标以 JSON 格式存储。此外，您可以在选择的监控系统中通过 Amazon CloudWatch Logs 使用增强监测 JSON 输出。

要在 CloudWatch 控制面板上显示图表并创建告警，以便在指标超出定义的阈值时启动操作，您必须通过 CloudWatch Logs 在 CloudWatch 中创建指标筛选条件。有关详细说明，请参阅 [AWS re:Post 文章](#)，了解如何筛选“增强监控”CloudWatch Logs 以生成 Amazon RDS 的自动自定义指标。

以下示例说明了 Custom/RDS 命名空间中的自定义指标 `CPU.User`。此自定义指标是通过筛选来自 CloudWatch Logs 的 `cpuUtilization.user`“增强监控”指标创建的。



当该指标在 CloudWatch 存储库中可用时，您可以在 CloudWatch 控制面板中显示和分析该指标，应用进一步的数学和查询运算，并设置告警以监控此特定指标，并在观察到的值与定义的告警条件不一致时生成提醒。

# 事件、日志和审计跟踪记录

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，以及在值超出定义阈值时生成提醒，这些都是帮助您实现和维护 Amazon RDS 数据库实例的可靠性、可用性、性能及安全性的必要和最佳实践。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、日志文件和审计跟踪记录。

## Sections

- [Amazon RDS 事件](#)
- [数据库日志](#)
- [审核跟踪](#)

## Amazon RDS 事件

Amazon RDS 事件表示 Amazon RDS 环境中的更改。例如，当数据库实例状态从正在启动变为可用时，Amazon RDS 会生成事件 RDS-EVENT-0088 The DB instance has been started。Amazon RDS 将事件近乎实时地传输到 Amazon EventBridge。您可以通过 Amazon RDS 控制台、AWS CLI 命令 [describe-events](#) 或 Amazon RDS API 操作 [DescribeEvents](#) 访问事件。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)

Filter by alarms < 1 > ⚙️

Name	State	More options
ApplicationInsights/RDS-DBS/AWS/RDS/CPUUtilization/database-1/	OK	<a href="#">view</a>
ApplicationInsights/RDS-DBS/AWS/RDS/ReadLatency/database-1/	OK	<a href="#">view</a>
ApplicationInsights/RDS-DBS/AWS/RDS/WriteLatency/database-1/	OK	<a href="#">view</a>

### 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)

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。信息包括：

- 来源名称和来源类型；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"
- 与事件关联的消息；例如："Message": "Finished updating DB parameter group"
- 事件类别；例如："EventCategories": ["configuration change"]

有关完整参考，请参阅 Amazon RDS 文档中的 [Amazon RDS 事件类别和事件消息](#)。

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更改、配置更改、只读副本状态更改、备份和恢复事件、失效转移操作、故障事件、对安全组的修改以及许多其他通知。例如，如果您已设置只读副本数据库实例以提高数据库的性能和持久性，我们建议您监控与数据库实例关联的只读副本事件类别的 Amazon RDS 事件。这是因为诸如 RDS-EVENT-0057 Replication on the read replica was terminated 之类的事件表明您的只读副本不再与主数据库实例同步。向负责团队通报发生了此类事件可能有助于及时缓解问题。Amazon EventBridge 和其他 AWS 服务 [例如 AWS Lambda、Amazon Simple Queue Service ( Amazon SQS ) 和 Amazon Simple Notification Service ( 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。如果您使用 AWS CLI 或 Amazon RDS API 查看事件，则使用 describe-events 命令检索过去 14 天内的事件，如下所示。

```
$ 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"
  }
]
```

如果想长期存储事件，则无论是一直存储到指定的到期期限还是永久存储，您都可以使用 [CloudWatch Logs](#) 来记录有关 Amazon RDS 生成的事件的信息。要实施此解决方案，您可以使用 Amazon SNS 主题来接收 Amazon RDS 事件通知，然后调用 Lambda 函数将事件记录在 CloudWatch Logs 中。

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 Logs。CloudWatch Logs 与 Lambda 集成，并提供了一种便捷方法来记录事件信息，即使用 print 函数将信息输出到 stdout。
2. 通过订阅 Lambda 函数创建 SNS 主题（将协议设置为 Lambda），并将端点设置为您在上一步中创建的 Lambda 函数的 Amazon 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，请参阅 [AWS re:Post 文章](#)，了解如何让您的 Amazon 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。将目标设置为 ARN，然后选择您之前创建的 SNS 主题。根据您的要求设置来源类型和要包括的事件类别。有关更多信息，请参阅 Amazon RDS 文档中的 [订阅 Amazon RDS 事件通知](#)。

## 数据库日志

MySQL 和 MariaDB 数据库会生成日志，您可以访问这些日志进行审计和问题排查。这些日志是：

- [审计](#)：审计跟踪记录是一组记录服务器活动的记录。对于每个客户端会话，它都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，例如在服务器启动和关闭期间以及服务器运行时发生的错误、警告和注意事项。
- [常规](#)：此日志记录 mysqld 的活动，包括每个客户端的连接和断开连接活动，以及从客户端接收的 SQL 查询。当您怀疑出现错误并想确切了解客户端向 mysqld 发送了什么内容时，常规查询日志可能非常有用。
- [慢速查询](#)：此日志记录了花费很长时间才执行的 SQL 查询。

作为最佳实践，您应该[将数据库日志从 Amazon RDS 发布到 Amazon CloudWatch Logs](#)。通过 CloudWatch Logs，您可以对日志数据进行实时分析，将数据存储在高持久性存储中，并使用 CloudWatch Logs 代理管理数据。您可以从 Amazon RDS 控制台[访问和查看您的数据库日志](#)。您还可以使用 CloudWatch Logs Insights，通过交互方式搜索并分析 CloudWatch Logs 中的日志数据。以下示例说明了对审计日志的查询，该查询会检查 CONNECT 事件在日志中出现的次数、谁连接以及这些事件是从哪个客户端（IP 地址）连接的。审计日志中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
```

示例 Log Insights 查询显示，rdsadmin 每 5 分钟从 localhost 连接到数据库一次，总共连接了 22 次，如下图所示。这些结果表明，该活动源自内部 Amazon RDS 流程，例如监控系统本身。

CloudWatch > Logs Insights

## Logs Insights

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

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

Select log group(s)

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

```

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

```

Run query Cancel Save History

Queries are allowed to run for up to 15 minutes.

Logs Visualization Export results Add to dashboard

Showing 1 of 22 records matched

22 records (2.3 kB) scanned in 3.2s @ 6 records/s (746.057 B/s)

#	@user	@ip	counter
▼ 1	rdsadmin		22

Field Value

@ip

@user rdsadmin

counter 22

日志事件通常包含您想要统计的重要消息，例如有关与 MySQL 和 MariaDB 数据库实例关联的操作的警告或错误。例如，如果操作失败，则可能会发生错误并将其记录到错误日志文件中，如下所

示：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发生趋势。您可以[使用筛选条件从 Amazon RDS 日志创建自定义 CloudWatch 指标](#)，以启用对 Amazon RDS 数据库日志的自动监控，从而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告警。[例如](#)，为日志组 `/aws/rds/instance/database-1/error` 创建一个指标筛选条件，用于监控错误日志并搜索[特定模式](#)，例如 ERROR。将筛选模式设置为 ERROR，将指标值设置为 1。筛选条件将检测每条包含关键字 ERROR 的日志记录，并将每个包含“ERROR”的日志事件的计数增加 1。创建筛选条件后，您可以设置告警，以在 MySQL 或 MariaDB 错误日志中检测到错误时通知您。

要详细了解如何通过创建 CloudWatch 控制面板并使用 CloudWatch Logs Insights 来监控慢速查询日志和错误日志，请参阅博客文章 [Creating an Amazon CloudWatch dashboard to monitor Amazon RDS and Amazon Aurora MySQL](#)。

## 审核跟踪

审计跟踪记录（或审计日志）提供与 AWS 账户中安全相关的事件的时间顺序记录。其中包括 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了书面证据。在 Amazon RDS for MySQL 或 MariaDB 中，使用审计跟踪记录涉及：

- 监控数据库实例审计日志
- 监控 AWS CloudTrail 中的 Amazon RDS API 调用

对于 Amazon RDS 数据库实例，审计的目标通常包括：

- 为以下内容启用问责制：
  - 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，或者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行为

数据库审计跟踪记录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其无限访问权限？

MySQL 和 MariaDB 都通过使用 MariaDB 审计插件实现数据库实例审计跟踪记录功能。此插件会记录数据库活动，例如用户登录数据库和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，请参阅 Amazon RDS 文档中的 [MySQL 的 MariaDB 审计插件支持](#)。审计日志中的记录以插件定义的特定格式存储。您可以在 [MariaDB 服务器文档](#) 中找到有关审计日志格式的更多详细信息。

您的 AWS 账户的 AWS 云审计跟踪记录由 [AWS CloudTrail](#) 服务提供。CloudTrail 将 Amazon RDS 的 API 调用作为事件捕获。所有 Amazon RDS 操作都会记录。CloudTrail 提供了用户、角色或 AWS 服务在 Amazon RDS 中所执行操作的记录。事件包括在 AWS 管理控制台、AWS CLI、AWS SDK 和 API 中所执行的操作。

## 示例

在典型的审计场景中，您可能需要将 AWS CloudTrail 跟踪与数据库审计日志和 Amazon RDS 事件监控相结合。例如，您可能遇到的情况是，您的 Amazon RDS 数据库实例（例如 database-1）的数据库参数已修改，您的任务是确定谁进行了修改、更改了哪些内容以及更改发生的时间。

要完成任务，请执行以下步骤：

1. 列出发生在数据库实例 database-1 上的 Amazon RDS 事件，并确定类别 configuration change 中是否存在包含消息 Finished updating DB parameter group 的事件。

```
$ 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 在部署 database-1 的区域中，于在步骤 1 中发现的 Amazon RDS 事件前后的时间段内，[搜索 CloudTrail 事件](#)，其中 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"
}
```

CloudTrail 事件显示，AWS 账户 111122223333 中角色为 Role1 的用户 User1 于 2022-12-01 at 09:18:19 h 修改了数据库实例 database-1 使用的数据库参数组 mariadb10-6-test。修改了两个参数，并设置为以下值：

- innodb\_log\_buffer\_size = 8388612
- innodb\_write\_io\_threads = 8

## 其他 CloudTrail 和 CloudWatch Logs 功能

您可以通过在 CloudTrail 控制台中查看事件历史记录对过去 90 天内的操作和安全事故进行问题排查。要延长保留期并利用其他查询功能，您可以使用 [AWS CloudTrail Lake](#)。借助 AWS CloudTrail Lake，您可以在事件数据存储中保存事件数据长达七年。此外，此服务支持复杂的 SQL 查询，相比事件历史记录中的简单密钥值查询提供的视图，这些查询提供更深入、更可自定义的事件视图。

要监控您的审计跟踪记录、设置告警并在特定活动发生时收到通知，您需要 [将 CloudTrail 配置为跟踪记录发送到 CloudWatch Logs](#)。将跟踪记录存储为 CloudWatch Logs 后，您可以定义指标筛选条件

来评估日志事件以匹配字词、短语或值，并将指标分配给指标筛选条件。此外，您还可以创建根据您的指定的阈值和时间段生成的 CloudWatch 告警。例如，您可以配置告警，向负责的团队发送通知，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。

# 警报

就您的 IT 基础设施和 IT 服务的安全性、可用性、性能和可靠性而言，提醒是最重要的信息来源之一。它们会通知 IT 团队有关持续存在的安全威胁、服务中断、性能问题或系统故障等情况。

信息技术基础设施库 (ITIL)，特别是 IT 服务管理 (ITSM) 实践，可将自动提醒设置为监控和活动管理及事件管理最佳实践的焦点。

事件提醒是指监控工具生成提醒，以通知您的团队和自动化工具 (对于可自动操作的项目) 有关 IT 环境中的更改、高风险操作或故障。IT 提醒是防止系统中断或更改演变成重大事件的第一道防线。通过自动监控系统并生成中断和风险更改提醒，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，Well-Architected Framework 规定您可以使用监控来生成基于警报的通知，并主动进行监控和警报。](#) AWS 使用 CloudWatch 或第三方监控服务设置警报，以指示指标何时超出预期界限。

提醒管理的目的是建立高效、标准化的程序，通过日志记录、分类、操作定义和实施、关闭和事后审查活动来处理与 IT 相关的活动和事件。

## Sections

- [CloudWatch 警报](#)
- [EventBridge 规则](#)
- [指定操作、启用和禁用告警](#)

## CloudWatch 警报

在操作 Amazon RDS 数据库实例时，您需要监控不同类型的指标、事件和跟踪并生成提醒。对于 MySQL 和 MariaDB 数据库，关键的信息来源是[数据库实例指标](#)、[操作系统指标](#)、[事件](#)、[日志和审计跟踪记录](#)。我们建议您使用[CloudWatch 警报](#)来监视您指定的时间段内的单个指标。

以下示例说明如何设置告警，监视所有 Amazon RDS 数据库实例的 CPUUtilization 指标 (CPU 利用率百分比)。您可以将告警配置为：任何数据库实例的 CPU 利用率在 5 分钟的评估期内超过 80% 时触发。

CloudWatch > Alarms > Create alarm

Step 1  
Specify metric and conditions

Step 2  
Configure actions

Step 3  
Add name and description

Step 4  
Preview and create

## Specify metric and conditions

### Metric

Graph

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

Percent

10.47

10.11

9.75

12:00 13:00 14:00

● CPUUtilization

Namespace  
AWS/RDS

Metric name  
CPUUtilization

Statistic  
Average

Period  
5 minutes

### Conditions

Threshold type

Static  
Use a value as a threshold

Anomaly detection  
Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition.

Greater  
> threshold

Greater/Equal  
>= threshold

Lower/Equal  
<= threshold

Lower  
< threshold

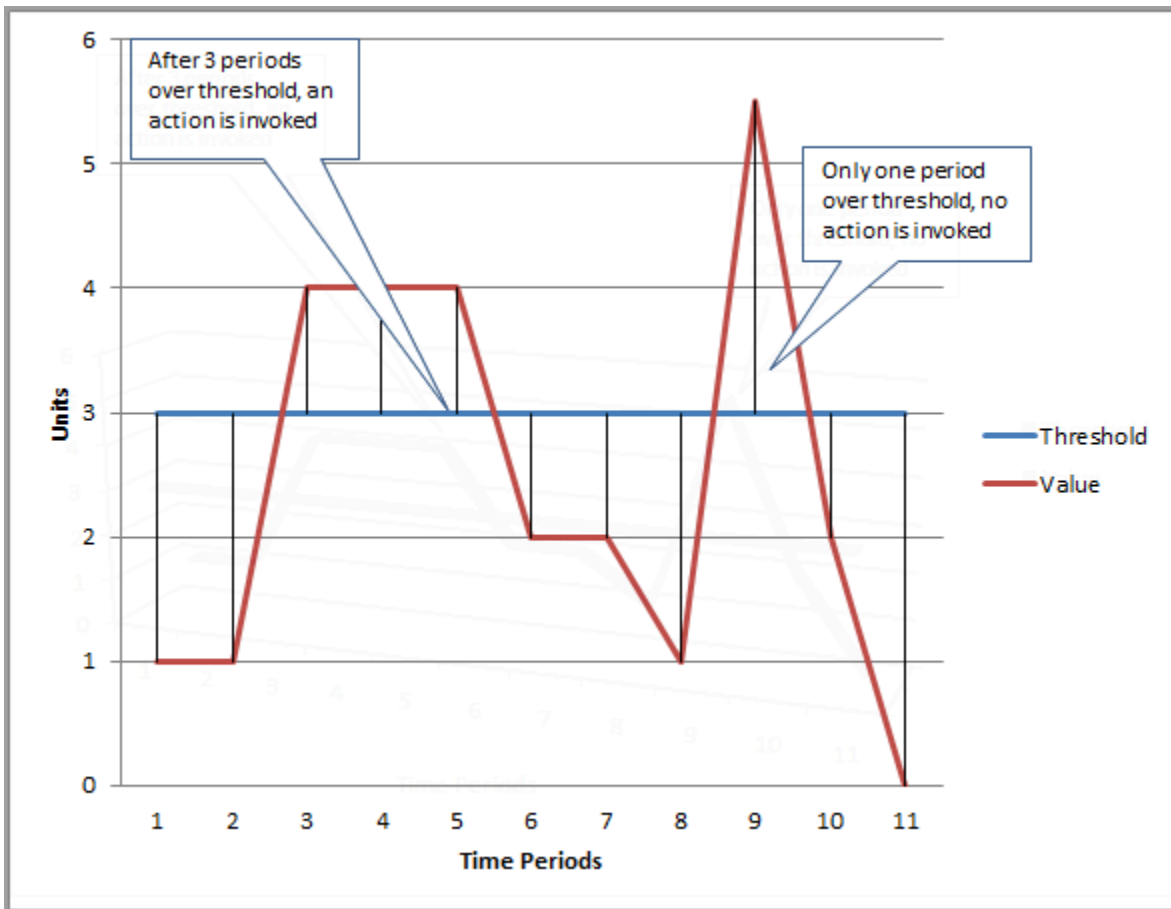
than...

Define the threshold value.

80

Must be a number

这意味着，如果您的任何数据库在 5 分钟或更长时间内出现高 CPU 利用率（超过 80%），告警就会进入 ALARM 状态。如果 CPU 在短时间内偶尔爆发增至 80% 以上的利用率，然后再次降至阈值以下，则告警将保持 OK 状态。下图说明了此逻辑。



CloudWatch 警报支持指标和复合警报。

- 指标警报监视单个 CloudWatch 指标，并且可以对该指标执行数学表达式。指标告警可以发送 Amazon SNS 消息，而 Amazon SNS 消息可以根据指标值相对于给定阈值在多个时间段内的值，执行一项或多项操作。
- 复合告警基于规则表达式，该表达式评估多个告警的状态，并且只有在满足规则的所有条件时才会进入 ALARM 状态。复合告警通常用于减少不必要的提醒数量。例如，您可能有一个复合告警，其中包含多个配置为从不执行操作的指标告警。当组合中的所有单个指标告警都已包含在 ALARM 中时，复合告警将发送提醒

CloudWatch 警报只能监视 CloudWatch 指标。如果要根据错误、慢速查询或一般日志创建警报，则必须从日志中创建 CloudWatch 指标。如前面的[操作系统监控和事件、日志和审计跟踪记录](#)部分所述，您可以使用筛选条件[根据日志事件创建指标](#)，来实现这一点。同样，要对增强监控指标发出警报，必须在“CloudWatch 日志” CloudWatch 中创建指标筛选器。

## EventBridge 规则

[Amazon RDS 事件](#)将传送到亚马逊 EventBridge，您可以使用[EventBridge 规则](#)对这些事件做出反应。例如，您可以创建 EventBridge 规则，以便在一个特定的数据库实例停止或启动时通知您并采取行动，如以下屏幕所示。

The screenshot shows the Amazon EventBridge console interface. On the left is a navigation sidebar with categories like Developer resources, Buses, Pipes, and Integration. The main content area is titled 'Rules' and includes a 'Select event bus' dropdown set to 'default'. Below that, there's a 'Rules (2/17)' section with a search bar containing 'rds', showing 2 matches. A table lists the rules:

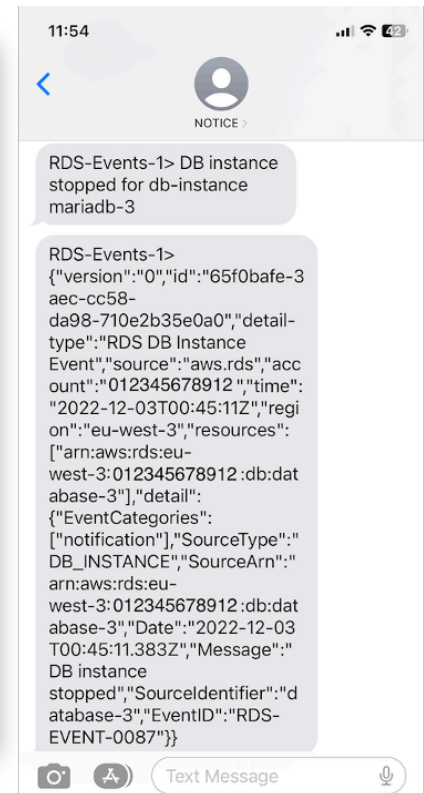
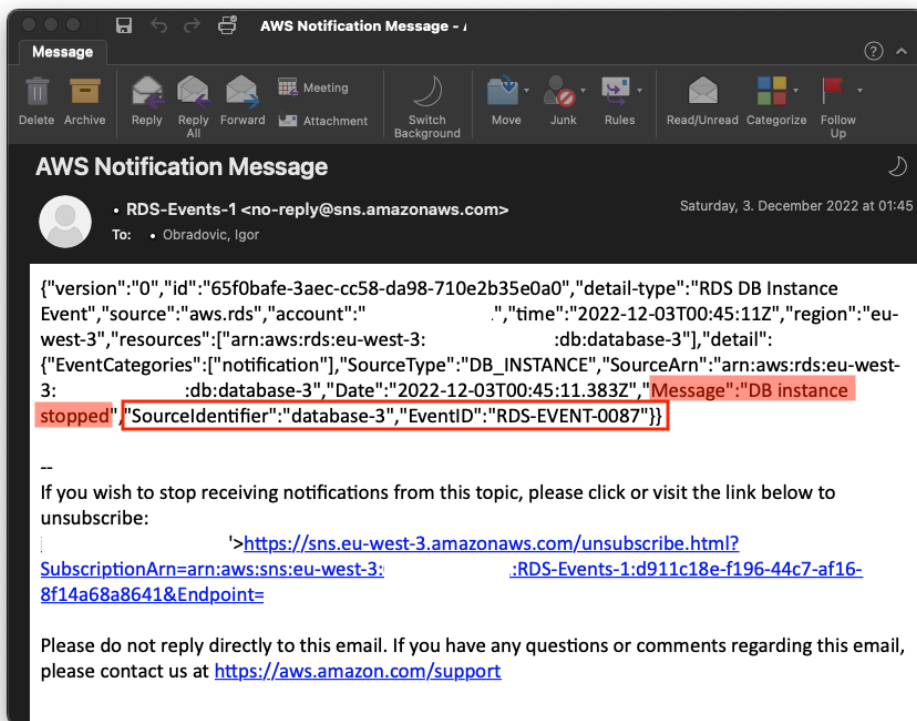
<input type="checkbox"/>	Name	Status	Type	Description
<input type="checkbox"/>	rds-shutdown-database-3	Enabled	Standard	
<input type="checkbox"/>	rds-startup-database-3	Enabled	Standard	

检测 The DB instance has been stopped 事件的规则具有 Amazon RDS 事件 ID RDS-EVENT-0087，因此您可以将该规则的 Event Pattern 属性设置为：

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

此规则仅监控数据库实例 database-3，并监视 RDS-EVENT-0087 事件。当 EventBridge 检测到该事件时，它会将事件发送到资源或终端节点（称为[目标](#)）。在这里，您可以指定在 Amazon RDS

实例关闭时要执行的操作。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) Simple Queue 队列、AWS Lambda 函数、AWS Systems Manager 自动化、作业、Amazon AWS Batch API Gateway 等。例如，您可以创建一个 SNS 主题来发送通知电子邮件和短信，并将该 SNS 主题指定为规则的 EventBridge 目标。如果 Amazon RDS 数据库实例 database-3 已停止，Amazon RDS 会 RDS-EVENT-0087 将事件传送到 EventBridge，然后在那里检测到该事件。EventBridge 然后调用目标，即 SNS 话题。SNS 主题配置为发送电子邮件 (如下图所示) 和 SMS。



## 指定操作、启用和禁用告警

您可以使用 CloudWatch 警报来指定警报在 OKALARM、和 INSUFFICIENT\_DATA 状态之间发生变化时应采取的操作。CloudWatch 内置了与 SNS 主题和几个不适用于 Amazon RDS 指标的其他操作类别的集成，例如亚马逊弹性计算云 (Amazon EC2) 操作或 Amazon EC2 Auto Scaling 群组操作。EventBridge 通常用于编写规则和定义在 Amazon RDS 指标触发警报时采取行动的目标。CloudWatch EventBridge 每当 CloudWatch 警报改变其状态时，都会向发送事件。您可以使用这些警报状态更改事件来触发中的事件目标 EventBridge。有关更多信息，请参阅 [警报事件和 EventBridge](#) CloudWatch 文档。

您可能还需要管理告警；例如，在计划的配置更改或测试期间自动禁用告警，然后在计划的操作结束后重新启用告警。例如，如果您有计划的、预定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，则可以使用中的 API 操作和或 [DisableAlarmActions](#) 和 [EnableAlarmActionsenable-alarm-actions](#) 命令来禁用 [disable-alarm-actions](#) 和启用警报 AWS CLI。您也可以在 CloudWatch 控制台上查看警报的历史记录，也可以使用 [DescribeAlarmHistory](#) API 操作或中的 [describe-alarm-history](#) 命令来查看警报的历史记录 AWS CLI。CloudWatch 将警报历史记录保存两周。在 CloudWatch 主机上，您可以在导航窗格中选择“收藏夹和最近”菜单，以设置和访问您最喜欢的警报和最近访问的警报。

## 后续步骤和资源

有关将关系数据库迁移到 AWS 云的更多信息，请参阅 AWS 规范指引网站上的以下策略：

- [关系数据库的迁移策略](#)

您可以在 [AWS 规范指引](#) 中探索数据库迁移模式，了解有关在 AWS 云中运行的特定关系数据库的分步说明，包括与监控、迁移和数据管理相关的任务。

有关其他资源，请参阅以下资源：

- [Amazon Relational Database Service 用户指南](#)
- [Amazon CloudWatch 用户指南](#)
- [Amazon RDS 常见问题](#)
- [性能详情常见问题](#)
- [Deliver Amazon RDS Performance Insights counter metrics to a third-party Application Performance Monitoring service provider using Amazon CloudWatch Metrics Stream](#) ( AWS 博客文章 )
- [Creating an Amazon CloudWatch dashboard to monitor Amazon RDS and Amazon Aurora MySQL](#) ( AWS 博客文章 )
- [Tuning Amazon RDS for MySQL with Performance Insights](#) ( 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
<a href="#">更新了有关性能详情的信息</a>	使用最新信息更新了 <a href="#">有关向 CloudWatch 发布性能详情指标的部分</a> 。	2025 年 3 月 11 日
<a href="#">更新了有关导出程序的信息</a>	更新了 <a href="#">有关导出程序的信息</a> ，并添加了选择导出程序的准则。	2024 年 6 月 13 日
<a href="#">初次发布</a>	—	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：将本地 Oracle 数据库迁移到 AWS 云中的 Amazon Relational Database Service ( Amazon RDS ) for Oracle。
- **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。
- **重新托管 ( 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：将本地 Oracle 数据库迁移到 AWS 云中 EC2 实例上的 Oracle。
- **重新放置 ( 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。您将服务器从本地平台迁移到同一平台的云服务中。示例：将 Microsoft Hyper-V 应用程序迁移到 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

请参阅[托管服务](#)。

## ACID

请参阅[原子性、一致性、隔离性、持久性](#)。

## 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。它比[主动-被动迁移](#)更灵活，但工作量更大。

## 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

一种 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

请参阅[人工智能](#)。

## AIOps

请参阅[人工智能运营](#)。

## 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？](#)

## 人工智能操作 (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 AIOps AWS 迁移策略中使用的更多信息，请参阅[操作集成指南](#)。

## 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 (IAM) [文档](#) [AWS 中的 AB AC](#)。

## 权威数据来源

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来源复制到其他位置，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

### 恶意机器人

一种旨在扰乱或伤害个人或组织的[机器人](#)。

### BCP

请参阅[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。另请参阅[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应用程序版本 ( 蓝色 )，在另一个环境中运行新应用程序版本 ( 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交互的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的 Web 爬网程序。还有一些被称为恶意机器人的机器人，其目的是扰乱或伤害个人或组织。

## 僵尸网络

被[恶意软件](#)感染并受单方（称为僵尸网络控制者或僵尸网络操作者）控制的[僵尸网络](#)。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）。

## 紧急（break-glass）访问

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 AWS Well-Architected Guidance 中的[Implement break-glass procedures](#) 指示器。

## 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

请参阅[AWS 云采用框架](#)。

## 金丝雀部署

缓慢而渐进地向最终用户发布版本。当您确信无误后，即可部署新版本，并完全替换当前版本。

## CCoE

请参阅[云卓越中心](#)。

## CDC

请参阅[更改数据捕获](#)。

## 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韧性。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

请参阅[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。云计算通常连接到[边缘计算](#)技术。

## 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 云中时通常会经历四个阶段：

- 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，创建着陆区、定义 CCo E、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 AWS 云企业战略博客的博客文章 [《云优先之旅和采用阶段》](#) 中定义了这些阶段。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

请参阅 [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 Bitbucket Cloud。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 管线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 )

一种 [AI](#) 领域，它使用机器学习来分析和提取数字图像和视频等视觉格式中的信息。例如，Amazon SageMaker AI 为 CV 提供了图像处理算法。

## 配置偏移

对于工作负载而言，一种偏离预期状态的配置更改。这可能会导致工作负载变得不合规，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，以自定义您的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、提高生产力、提高代码质量和更快地交付。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

请参阅[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-Architected 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 云 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

请参阅[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。

## 委派管理员

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。此帐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

请参阅[环境](#)。

## 侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出提醒。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

[星型架构](#)中的一种较小的表，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 )

您用来最大程度地减少由[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 Framework AWS work 中的“[工作负载灾难恢复：云端 AWS 恢复](#)”。

## DML

请参阅[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

请参阅[灾难恢复](#)。

## 偏差检测

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

请参阅[开发价值流映射](#)。

## E

### EDA

请参阅[探索性数据分析](#)。

### EDI

请参阅[电子数据交换](#)。

## 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](#)比较时，边缘计算可以减少通信延迟并缩短响应时间。

## 电子数据交换 ( EDI )

组织之间业务文件的自动交换。有关更多信息，请参阅[什么是电子数据交换](#)。

## 加密

一种将人类可读的纯文本数据转换为加密文字的计算流程。

## 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

请参阅[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](#)。

## 环境

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

请参阅[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 and 创建数据可视化得以执行。

# F

## 事实表

[星型架构](#)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。

## 快速失效机制

一种使用频繁且增量式的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 云，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

请参阅[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，请参阅使用[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。

## 少样本提示

在要求 [LLM](#) 执行类似任务之前，先向其提供少量示例，以演示任务和预期输出。此技术是上下文内学习的一种应用，其中模型可以从提示中嵌入的示例 ( 样本 ) 中学习。对于需要特定格式、推理或领域知识的任务，少样本提示可能非常有效。另请参阅[零样本提示](#)。

## FGAC

请参阅[精细访问控制](#)。

## 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，通过[更改数据捕获](#)使用连续数据复制，在极短的时间内迁移数据，而非使用分阶段方法。目标是将停机时间降至最低。

## FM

请参阅[基础模型](#)。

## 基础模型 ( FM )

一个大型深度学习神经网络，一直在广义和未标记数据的大量数据集上进行训练。FMs 能够执行各种各样的一般任务，例如理解语言、生成文本和图像以及用自然语言进行对话。有关更多信息，请参阅[什么是基础模型](#)。

# G

## 生成式人工智能

[AI](#) 模型的一个子集，这些模型已经过大量数据训练，可以使用简单的文本提示来创建新的内容和构件，例如图像、视频、文本和音频。有关更多信息，请参阅[什么是生成式人工智能](#)。

## 地理阻止

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工作流程，而[基于中继的工作流程](#)则是现代的、首选的方法。

### 黄金映像

系统或软件的快照，用作部署该系统或软件的新实例的模板。例如，在制造业中，黄金映像可用于在多个设备上预调配软件，并有助于提高设备制造操作的速度、可扩展性和生产效率。

### 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

帮助管理各组织单位的资源、策略和合规性的高级规则 (OUs)。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。侦测性护栏会检测策略违规和合规性问题，并生成提醒以进行修复。它们通过使用 AWS Config、Amazon、AWS Security Hub CSPM GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

## H

### HA

请参阅[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。

## 保留数据

从用于训练[机器学习](#)模型的数据集中保留的一部分标注的历史数据。通过将模型预测与保留数据进行比较，您可以使用保留数据来评估模型性能。

## 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。

## hypercure 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 hypercure 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。

# 我

## laC

请参阅[基础设施即代码](#)。

## 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 云环境中的权限。

## 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。

## IloT

请参阅[工业物联网](#)。

## 不可变基础设施

一种模型，可为生产工作负载部署新的基础设施，而不是更新、修补或修改现有基础设施。不可变基础设施本质上比[可变基础设施](#)更一致、更可靠、更可预测。有关更多信息，请参阅 AWS Well-Architected Framework 中的[使用不可变基础设施进行部署](#)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](#)建议设置您的网络帐户，包括入站、出站和检查，VPCs 以保护您的应用程序与更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 [Klaus Schwab](#) 在 2016 年提出，指的是通过连接、实时数据、自动化、分析和 AI/ML 的进步来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调配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 (IloT)

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 \(IloT\) 数字化转型战略](#)。

## 检查 VPC

在 AWS 多账户架构中，一种集中式 VPC，用于管理对 VPCs（相同或不同 AWS 区域）、互联网和本地网络之间的网络流量的检查。[AWS 安全参考架构](#)建议设置您的网络帐户，包括入站、出站和检查，VPCs 以保护您的应用程序与更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[机器学习模型的可解释性 AWS](#)。

## 物联网

请参阅[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](#)。

## 大语言模型 ( LLM )

一种基于大量数据进行预训练的深度学习 [AI](#) 模型。LLM 可以执行多项任务，例如回答问题、总结文档、将文本翻译成其他语言以及完成句子。有关更多信息，请参阅[什么是 LLMs](#)。

## 大规模迁移

迁移 300 台或更多服务器。

## LBAC

请参阅[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

请参阅 [7 R](#)。

## 小端序系统

一个先存储最低有效字节的系统。另请参阅[字节顺序](#)。

## LLM

请参阅[大型语言模型](#)。

## 下层环境

请参阅[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

请参阅[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权限。恶意软件的示例包括病毒、蠕虫、勒索软件、木马、间谍软件和键盘记录器。

## 托管式服务

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。Amazon Simple Storage Service ( Amazon S3 ) 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、记录和控制将原材料转化为成品的生产过程。

## MAP

请参阅[迁移加速计划](#)。

## 机制

一个完整的过程，您可以在其中创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运作过程中自我强化和改善的循环。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

请参阅[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

一种小型的独立服务，通过明确的定义进行通信 APIs ，通常由小型的独立团队拥有。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通过定义明确的接口进行通信。APIs 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、开发人员和冲刺 DevOps 领域的专业人员。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，提供了用于验证迁移到 AWS 云的业务案例的信息。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

将工作负载迁移到 AWS 云的方法。有关更多信息，请参见术语表中的 [7 R](#) 词条，以及[动员您的组织以加快大规模迁移](#)。

## ML

请参阅[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 and 利用创新。有关更多信息，请参阅[在 AWS 云中实现应用程序现代化的策略](#)。

## 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。有关更多信息，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

请参阅[迁移组合评测](#)。

## 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？”

## 可变基础设施

一种用于更新和修改生产工作负载的现有基础设施的模型。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[来源访问控制](#)。

### OAI

请参阅[来源访问身份](#)。

### OCM

请参阅[组织变革管理](#)。

## 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

请参阅[运营集成](#)。

### OLA

请参阅[运营级别协议](#)。

## 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

请参阅[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 提供了一个包含数据加密、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 )

一份问题核对清单和关联的最佳实践，可帮助您了解、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 [AWS Well-Architected Framework 中的运营准备情况审查 \( ORR \)](#)。

## 运营技术 ( 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](#) 转型的关键重点。

## 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 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 )

在中 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。

## ORR

请参阅[运营准备情况审查](#)。

## OT

请参阅[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](#)建议设置您的网络帐户，包括入站、出站和检查，VPCs 以保护您的应用程序与更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

请参阅[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

请参阅[可编程逻辑控制器](#)。

## PLM

请参阅[产品生命周期管理](#)。

## policy

一个对象，可以定义权限 ( 请参阅[基于身份的策略](#) )、指定访问条件 ( 请参阅[基于资源的策略](#) ) 或定义 AWS Organizations 的组织中所有账户的最大权限 ( 请参阅[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。

## 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 false 的查询条件，通常位于 WHERE 子句中。

## 谓词下推

一种数据库查询优化技术，可在传输之前筛选查询中的数据。这将减少从关系数据库检索和处理的数据量，并提高查询性能。

## 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 文档中的[角色术语和概念](#)中的主体。

## 隐私设计

一种在整个开发过程中都考虑隐私的系统工程方法。

## 私有托管区

一个容器，其中包含有关您希望 Amazon Route 53 如何响应针对一个或多个 VPCs 域名及其子域名的 DNS 查询的信息。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](#)，旨在防止部署不合规资源。这些控制会在资源预置之前对其进行扫描。如果资源与控制不兼容，则不会预置它。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 )

对产品在其整个生命周期内的数据和流程的管理，从设计、开发和发布，到增长和成熟，再到衰退和淘汰。

### 生产环境

请参阅[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。

### 提示串接

使用一个 [LLM](#) 提示的输出作为下一个提示的输入，以生成更好的响应。该技术用于将复杂的任务分解为子任务，或者迭代地完善或扩展初步响应。它有助于提高模型响应的准确性和相关性，并允许获得更精细的个性化结果。

### 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。

## publish/subscribe (pub/sub)

一种支持微服务间异步通信的模式，可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

一系列用于访问 SQL 关系数据库系统中的数据的步骤，类似于指令。

### 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

请参阅[责任、问责、咨询和知情 \( RACI \)](#)。

## RAG

请参阅[检索增强生成](#)。

## 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

请参阅[责任、问责、咨询和知情 \( RACI \)](#)。

## RCAC

请参阅[行列访问控制](#)。

## 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

请参阅 [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

请参阅 [7 R](#)。

## Region

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[指定您的账户可以使用的 AWS 区域](#)。

## 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

请参阅 [7 R](#)。

## 版本

在部署过程中，推动生产环境变更的行为。

## 重新放置

请参阅 [7 R](#)。

## 更换平台

请参阅 [7 R](#)。

## 重新购买

请参阅 [7 R](#)。

## 韧性

应用程序抵御中断或从中断中恢复的能力。在 AWS 云中规划韧性时，[高可用性](#)和[灾难恢复](#)是常见的考虑因素。有关更多信息，请参阅 [AWS 云韧性](#)。

## 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

请参阅 [7 R](#)。

## 停用

请参阅 [7 R](#)。

## 检索增强生成 ( RAG )

一种[生成式人工智能](#)技术，其中 [LLM](#) 在生成响应之前引用其训练数据来源之外的权威数据来源。例如，RAG 模型可以对组织的知识库或自定义数据执行语义搜索。有关更多信息，请参阅[什么是 RAG](#)。

## 轮换

定期更新[密钥](#)以使攻击者更难访问凭证的过程。

## 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

请参阅[恢复点目标](#)。

## RTO

请参阅[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 管理控制台 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

请参阅[监督控制和数据采集](#)。

## SCP

请参阅[服务控制策略](#)。

## 机密密钥

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 Secrets Manager 文档中的[什么是 Amazon Secrets Manager 密钥？](#)。

## 安全设计

一种在整个开发过程中都考虑安全的系统工程方法。

## 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。安全控制有以下四种类型：[预防性](#)、[检测性](#)、[响应性](#)和[主动性](#)。

## 安全固化

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

一种预定义的程序化操作，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 实例或轮换凭证。

## 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，用于集中控制组织中所有账户的权限 AWS Organizations。SCPs 定义防护措施或限制管理员可以委托给用户或角色的操作。您可以使用 SCPs 允许列表或拒绝列表来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。

## 服务水平指示器 ( SLI )

对服务性能方面的衡量，例如错误率、可用性或吞吐量。

## 服务水平目标 ( SLO )

代表服务运行状况的目标指标，由[服务水平指示器](#)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](#)。

## SIEM

请参阅[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

请参阅[服务水平协议](#)。

## SLI

请参阅[服务水平指示器](#)。

## SLO

请参阅[服务水平目标](#)。

## 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[在 AWS 云中实现应用程序现代化的分阶段方法](#)。

## SPOF

请参阅[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事务数据或测量数据，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。

## 监督控制和数据采集 ( SCADA )

在制造业中，一种使用硬件和软件来监控实物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。您可以使用 [Amazon S CloudWatch ynthetic](#) 来创建这些测试。

## 系统提示

一种为 [LLM](#) 提供上下文、说明或准则以指导其行为的技术。系统提示有助于设置上下文并制定与用户交互的规则。

# T

## 标签

键值对，用作组织资源的元数据。AWS 标签有助于您管理、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

请参阅[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

一个网络传输中心，可用于将您的网络 VPCs 和本地网络互连。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。

## 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

请参阅[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

两者之间的连接 VPCs，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

一种对与当前记录有某种关联的一组行执行计算的 SQL 函数。窗口函数对于处理任务很有用，例如计算移动平均值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。

## WORM

请参阅[一次写入多次读取](#)。

## WQF

请参阅[AWS 工作负载资格鉴定框架](#)。

## 一次写入多次读取 ( WORM )

一种存储模型，可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，但无法对其进行更改。此数据存储基础设施被认为[不可变](#)。

# Z

## 零日漏洞利用

一种利用[零日漏洞](#)的攻击，通常为恶意软件。

## 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。

## 零样本提示

为[LLM](#)提供执行任务的说明，但没有可以帮助指导的示例（样本）。LLM 必须使用预先训练的知识来处理任务。零样本提示的有效性取决于任务的复杂性和提示的质量。另请参阅[少样本提示](#)。

## 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。