aws

用户指南

Amazon DevOps Guru

Amazon DevOps Guru: 用户指南

Table of Contents

什么是 Amazon DevOps Guru？ 1
DevOpsGuru 是如何工作的？ 1
高级 DevOps大师工作流程 1
详细的 DevOps Guru 工作流程 3
怎样入门？ 4
如何停止收取 DevOps Guru 费用？ 4
概念 5
异常 5
见解 5
指标和操作事件 5
日志组和日志异常 5
建议 6
涵盖 6
服务涵盖范围列表 7
设置 10
报名参加 AWS 10
注册获取 AWS 账户 10
创建具有管理访问权限的用户 11
确定 DevOps Guru 的覆盖范围 12
确定您的通知主题 13
添加到主题的权限 13
估算成本 15
开始使用 17
步骤 1：设置 17
第 2 步：启用 DevOps Guru 17
监控整个组织的账户 17
监控您的当前账户 19
第 3 步：指定您的 DevOps Guru 资源覆盖范围 20
为 DevOps Guru 分析启用 AWS 服务 22
使用见解 23
查看见解 23
在 DevOps Guru 控制台中了解见解 24
了解异常行为如何分组为见解 26
了解见解严重性 27

监控数据库 28
关系数据库 28
在 Amazon RDS 中监控数据库操作 28
监控中的数据库操作 Amazon Redshift 30
在 DevOps Guru 中处理 RDS 中的异常情况 31
非关系数据库 47
监控中的数据库操作 Amazon DynamoDB 47
监控中的数据库操作 Amazon ElastiCache 47
与 CodeGuru Profiler 集成 49
使用 AWS 资源定义应用程序 50
使用标签识别应用程序中的资源 50
什么是标签？ 51
使用标签来定义应用程序 52
在 DevOps Guru 中使用标签 52
将标签添加到资源 53
使用堆栈来识别 DevOps Guru 应用程序中的资源 53
选择要分析的堆栈 54
与 EventBridge 55
DevOpsGuru 活动 55
DevOps Guru New Insight 公开活动 55
针对高严重性的新见解自定义示例事件模式 57
更新设置 58
更新您的管理账户 58
更新您的 AWS 分析覆盖范围 58
更新您的通知 58
在 DevOps Guru 控制台中导航到通知设置 59
添加 Amazon SNS 通知主题 60
移除亚马逊 SNS 通知主题 60
更新 Amazon SNS 通知配置 60
添加到主题的权限 61
筛选您的通知 62
使用 Amazon SNS 订阅筛选策略来筛选通知 62
筛选出来的 Amazon SNS 通知示例 63
更新 Systems Manager 集成 64
更新日志异常检测 65
更新加密 65

查看通知 67
新见解 67
已关闭见解 68
新关联 70
新建议 71
严重性升级 72
资源验证失败 73
查看已分析的资源 74
更新您的 AWS 分析覆盖范围 74
为用户移除已分析资源的视图 76
最佳实践 77
安全性 78
数据保护 78
数据加密 79
DevOpsGuru 如何使用补助金 AWS KMS 80
在 DevOps Guru 中监控您的加密密钥 81
创建客户托管密钥 81
流量隐私 83
身份和访问管理 83
受众 83
使用身份进行身份验证 84
使用策略管理访问 85
策略更新 86
Amazon DevOps Guru 如何与 IAM 合作 90
基于身份的策略 95
使用服务关联角色 105
DevOpsGuru 权限参考 111
Amazon SNS 主题的权限 115
加密的 Amazon SNS 主题的权限 118
问题排查 118
监控 DevOps大师 122
使用监控 CloudWatch 123
使用记录 DevOps Guru API 调用 AWS CloudTrail 125
VPC 端点（AWS PrivateLink） 128
DevOpsGuru VPC 终端节点的注意事项 128
为 DevOps Guru 创建接口 VPC 终端节点 128

为 DevOps Guru 创建 VPC 终端节点策略 128
基础结构安全性 129
恢复能力 130
限额和限制 131
通知 131
CloudFormation 堆栈 131
DevOpsGuru 资源监控限制 131
DevOps创建、部署和管理 API 的大师配额 131
文档历史记录 133
AWS 词汇表 138
..... cxxxix

什么是 Amazon DevOps Guru？

欢迎阅读 Amazon DevOps Guru 用户指南。

DevOpsGuru 是一项完全托管的运营服务，可让开发人员和操作员轻松提高其应用程序的性能和可用性。 DevOpsGuru 可以让你卸下与识别操作问题相关的管理任务，这样你就可以快速实施改进应用程序的建议。 DevOpsGuru 创建了反应式见解，您可以立即使用这些见解来改进您的应用程序。它还可以提供主动见解，帮助您避免将来可能影响应用程序的操作问题。

DevOpsGuru 应用机器学习来分析您的运营数据以及应用程序指标和事件，以识别偏离正常操作模式的行为。当 DevOps Guru 检测到操作问题或风险时，您会收到通知。对于每个问题， DevOpsGuru都会提出明智的建议，以解决当前和预测的未来运营问题。

要了解其用法，请参阅 我该如何开始使用 DevOps Guru？

DevOpsGuru 是如何工作的？

DevOpsGuru 工作流程从您配置覆盖范围和通知时开始。设置 DevOps Guru 后，它会开始分析您的运营数据。当它检测到异常行为时，它会创建包含建议以及与问题相关的指标、日志组和事件列表的见解。对于每一个见解， DevOpsGuru 都会通知你。如果您启用 AWS Systems Manager OpsCenter，OpsItem 则会创建一个，这样您就可以使用 Systems Manager OpsCenter 来跟踪和管理处理您的见解。每个见解都包含与异常行为相关的建议、指标、日志组和事件。使用见解中的信息来帮助您了解和解决异常行为。

有关三个高级工作流程步骤的更多详细信息，请参阅 高级 DevOps大师工作流程。请参阅详细的 DevOps Guru 工作流程，了解更详细的 DevOps Guru 工作流程，包括它如何与其他 AWS 服务交互。

主题

- 高级 DevOps大师工作流程
- 详细的 DevOps Guru 工作流程

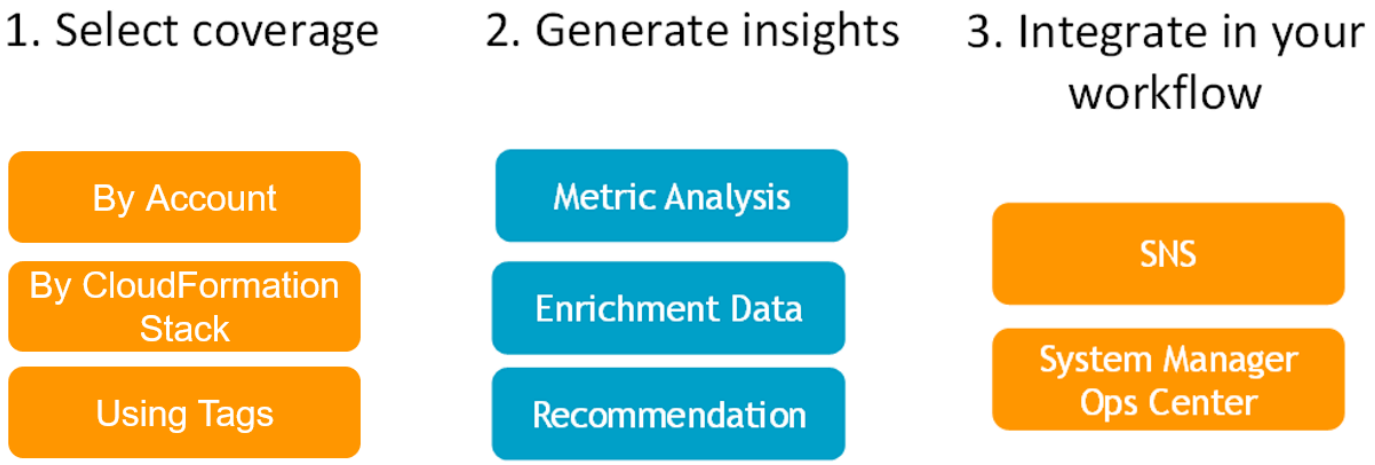
高级 DevOps大师工作流程

Amazon DevOps Guru 的工作流程可以分为三个高级步骤。

1. 告诉 DevOps Guru 要分析您 AWS 账户中的哪些 AWS 资源，从而指定 Guru 的覆盖范围。
2. DevOpsGuru 开始分析 Amazon CloudWatch 指标和其他运营数据 AWS CloudTrail，以确定可以修复的问题，从而改善您的运营。

3. DevOpsGuru 通过向您发送每个重要的 DevOps Guru 事件的通知，确保您了解见解和重要信息。

您还可以将 DevOps Guru 配置为创建 OpsItem 输入 AWS Systems Manager OpsCenter 以帮助您跟踪见解。下图演示了此高级工作流程。

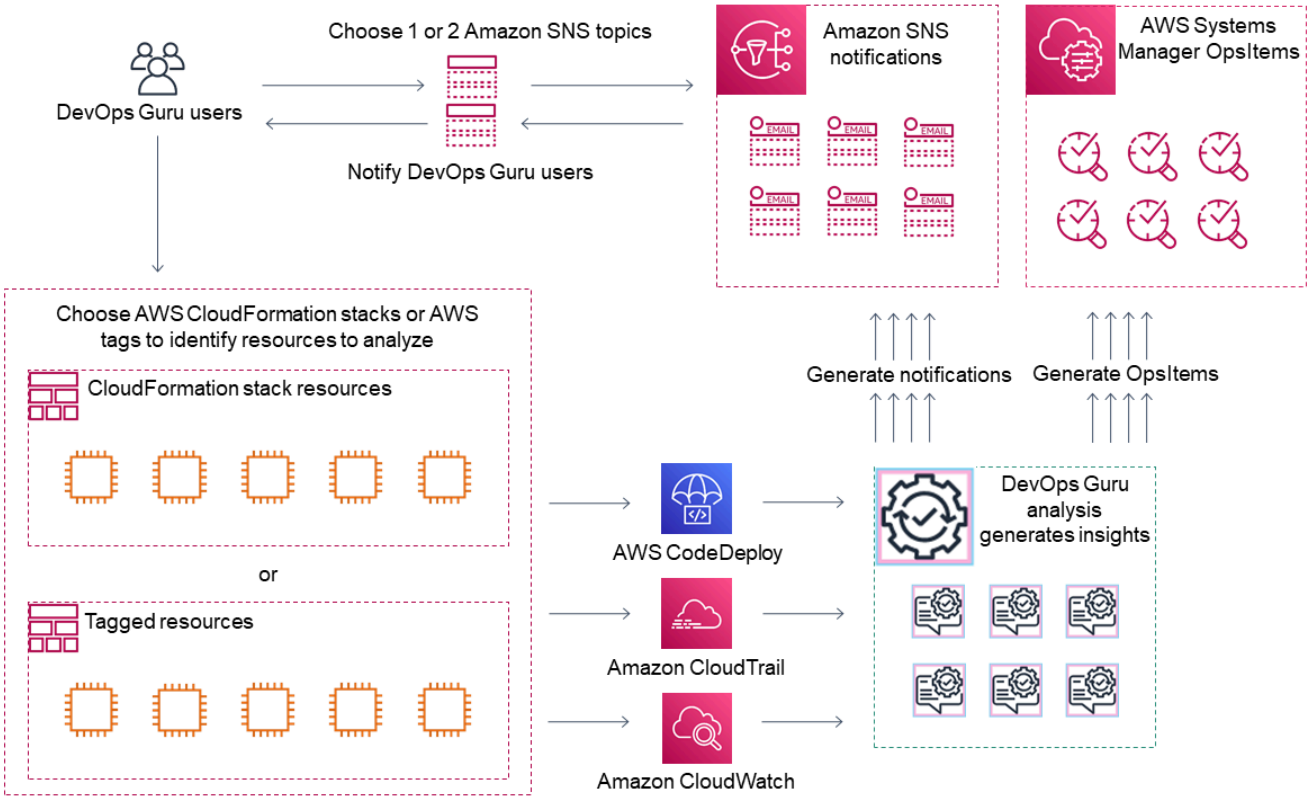


1. 在第一步中，您可以通过指定要分析您 AWS 账户中的哪些 AWS 资源来选择覆盖范围。DevOpsGuru 可以覆盖或分析 AWS 账户中的所有资源，也可以使用 AWS CloudFormation 堆栈或 AWS 标签来指定账户中要分析的资源子集。确保您指定的资源构成您的关键业务应用程序、工作负载和微服务。有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。
2. 在第二步中， DevOpsGuru 分析资源以生成见解。这是一个持续的过程。您可以在 DevOps Guru 控制台中查看见解并查看其中包含的建议和相关信息。 DevOps Guru 分析以下数据以发现问题并提供见解。
   - 您的 AWS 资源发出的各个 Amazon CloudWatch 指标。发现问题后， DevOpsGuru 会将这些指标汇总在一起。
   - 记录来自 Ama CloudWatch zon 日志组的异常情况。如果您启用日志异常检测，DevOpsGuru 会在问题发生时显示相关的日志异常。
   - DevOpsGuru 从 AWS CloudTrail 管理日志中提取丰富数据，以查找与收集的指标相关的事件。这些事件可以是资源部署事件和配置更改。
   - 如果您使用 AWS CodeDeploy， DevOpsGuru 会分析部署事件以帮助生成见解。对所有类型的 CodeDeploy 部署（本地服务器、亚马逊 EC2 服务器、Lambda 或 Amazon EC2）的事件进行分析。
   - 当 DevOps Guru 发现特定模式时，它会生成一个或多个建议，以帮助缓解或修复已发现的问题。这些建议是在一个见解中收集的。该见解还包含与问题相关的指标和事件的列表。您可以使用见解数据来解决和了解已发现的问题。

3. 在第三步中， DevOpsGuru 将洞察通知集成到您的工作流程中，以帮助您管理问题并快速解决问题。
   - 在您的 AWS 账户中生成的见解将发布到 Guru 设置期间选择 DevOps的亚马逊简单通知服务 (Amazon SNS) Service 主题。这是在创建见解后立即通知您的方式。有关更多信息，请参阅 在 DevOps Guru 中更新你的通知。
   - 如果您在 DevOps Guru 设置 AWS Systems Manager 期间启用，则每个见解都会创建相应的见解 OpsItem 来帮助您跟踪和管理发现的问题。有关更多信息，请参阅 在 DevOps Gur AWS Systems Manager u 中更新集成。

详细的 DevOps Guru 工作流程

DevOpsGuru 工作流程与多项 AWS 服务集成，包括亚马逊 CloudWatch AWS CloudTrail、、亚马逊简单通知服务和 AWS Systems Manager。下图显示了详细的工作流程，其中包括如何与其他 AWS 服务配合使用。



此图显示了一种场景，在该场景中， DevOpsGuru 的覆盖范围由 AWS CloudFormation 堆栈中定义的 AWS 资源或使用 AWS 标签来指定。如果未选择堆栈或标签， DevOpsGuru 覆盖率将分析您账户中的所有 AWS 资源。有关更多信息，请参阅使用 AWS 资源定义应用程序和确定 DevOps Guru 的覆盖范围。

1. 在设置过程中，您可以指定一两个 Amazon SNS 主题，这些主题用于通知您重要的 DevOps Guru 事件，例如创建洞察的时间。接下来，您可以指定 AWS CloudFormation 堆栈来定义要分析的资源。您还可以让 Systems Manager OpsItem 为每个见解生成一个，以帮助您管理见解。
2. 配置 DevOps Guru 后，它会开始分析从您的资源中发出的 CloudWatch 指标、日志组和事件以及与指标相关的 AWS CloudTrail 数据。 CloudWatch如果您的操作包括 CodeDeploy 部署，DevOpsGuru 还会分析部署事件。

   DevOps当Guru在分析的数据中识别出异常的异常行为时，它就会产生见解。每个见解都包含一个或多个建议、用于生成见解的指标列表、相关日志组列表以及用于生成见解的事件列表。使用此信息来解决已发现的问题。
3. 创建每个见解后， DevOpsGuru 都会使用 Amazon SNS 主题或在 Guru 设置 DevOps期间指定的主题发送通知。如果你启用 DevOps Guru 在 Systems Manager OpsItem 中生成一个 OpsCenter，那么每个见解也会触发一个新的系统管理器OpsItem。您可以使用 Systems Manager 来管理您的见解 OpsItems。

我该如何开始使用 DevOps Guru？

我们建议您完成以下步骤：

1. 阅读中的信息，了解有关 DevOps Guru 的更多信息。DevOps大师概念
2. 按照中的步骤@@ 设置您的 AWS 帐户 AWS CLI、和管理用户设置 Amazon DevOps Guru。
3. 按照中的DevOpsGuru 入门说明@@ 使用 DevOps Guru。

如何停止收取 DevOps Guru 费用？

要禁用 Amazon DevOps Guru，使其停止因分析您的 AWS 账户和地区的资源而产生费用，请更新您的覆盖范围设置，使其不分析资源。为此，请按照 在 DevOps Guru 中更新你的 AWS 分析覆盖范围中的步骤操作，然后在步骤 4 中选择 “无”。您必须为 DevOps Guru 分析资源的每个 AWS 账户和地区执行此操作。

> **Note**
>
> 如果您更新报道以停止分析资源，则如果您查看 DevOps Guru过去生成的现有见解，则可能会继续产生少量费用。这些费用与用于检索和显示见解信息的 API 调用有关。有关更多信息，请参阅 Amazon DevOps Guru 定价。

DevOps大师概念

以下概念对于理解 Amazon DevOps Guru 的工作原理非常重要。

主题

- 异常
- 见解
- 指标和操作事件
- 日志组和日志异常
- 建议

异常

异常表示 DevOps Guru 检测到的一个或多个意外或异常的相关指标。 DevOpsGuru 使用机器学习来分析与您的资源相关的指标和运营数据，从而生成异常。 AWS 在设置 Amazon DevOps Guru 时，您可以指定要分析的 AWS 资源。有关更多信息，请参阅 设置 Amazon DevOps Guru。

见解

见解是在您设置 Guru 时对您指定的 AWS 资源进行分析时创建的一系列异常。 DevOps每项见解都包含可用于改善操作性能的观察结果、建议和分析数据。有两种类型的见解：

- 被动见解：可在异常行为发生时识别此类行为。它包含异常以及建议、相关指标和事件，可帮助您立即了解和解决问题。
- 主动见解：可以让您在问题发生之前了解问题行为。它包含了带有建议的异常情况，以帮助您在问题预计发生之前采取措施。

指标和操作事件

构成见解的异常是通过分析 Amazon 返回的指标 CloudWatch 和您的资源发出的操作事件生成的。 AWS 您可以查看指标和操作事件，从而获得见解，从而帮助您更好地了解应用程序中的问题。

日志组和日志异常

启用日志异常检测后，相关的日志组将显示在 Guru 控制台的 DevOps Guru Insight 页面上。 DevOps 日志组可让您了解有关资源运行和访问方式的关键诊断信息。

日志异常表示在日志组中发现的类似异常日志事件的集群。可能在 DevOps Guru 中显示的异常日志事件的示例包括关键字异常、格式异常、HTTP 代码异常等。

您可以使用日志异常来诊断操作问题的根本原因。 DevOpsGuru 还在洞察建议中引用日志行，为推荐的解决方案提供更多背景信息。

> **Note**
>
> DevOpsGuru 与 Amazon CloudWatch 合作启用日志异常检测。启用日志异常检测后，DevOpsGuru 会向您的 CloudWatch 日志组添加标签。当您关闭日志异常检测时，DevOpsGuru 会从您的 CloudWatch 日志组中删除标签。
> 此外，管理员应确保只有有权查看 CloudWatch 日志的用户才有权查看异常 CloudWatch 日志。我们建议您使用 IAM Policy 允许或拒绝对 `ListAnomalousLogs` 操作的访问。有关更多信息，请参阅 DevOpsGuru 的 Identity and Access 管理。

建议

每个见解均提供建议，其中包括帮助您提高应用程序性能的建议。建议包括以下内容：

- 解决构成该见解的异常的建议操作说明。
- DevOpsGuru 发现异常行为的分析指标清单。每个指标都包括生成与指标关联的资源的 CloudFormation 堆栈的名称、资源的名称以及与该资源关联的 AWS 服务的名称。
- 与该见解相关的异常指标的事件列表。每个相关事件都包含生成与该事件关联的资源的 CloudFormation 堆栈的名称、生成该事件的资源名称以及与该事件关联的 AWS 服务的名称。
- 与见解相关的异常行为相关的日志组列表。每个日志组都包含一条示例日志消息、有关报告的日志异常类型的信息、日志异常发生的时间以及查看日志行的链接。 CloudWatch

DevOps大师报道

DevOpsGuru 探讨了许多不同的 AWS 服务并提供了见解。对于 DevOps Guru为其创建见解的每项服务，DevOpsGuru都会显示各种分析指标和生成的见解。

被动见解的示例使用案例：

服务名称	使用场景	示例	指标
AWS Lambda	检测由各种根本原因（例如冷启动、请求增加、下游节流或代码部署）引起的 Lambda 函数的延迟或持续时间异常。推荐快速缓解的方法。	代码部署： Amazon API Gateway 延迟受最近部署 Lambda 代码后的 Lambda 延迟增加的影响。下游节流：操作员减少了 DynamoDB 读取单元的容量，导致重试次数增加。这会导致节流。冷启动：Lambda 函数的配置不足，因此 Lambda 在发出请求时需要更长时间。	持续时间 节流

主动见解的示例使用案例：

服务名称	使用场景	指标
Amazon DynamoDB	DynamoDB 表读取消耗容量存在达到表限值的风险。建议的操作：如果使用预置容量模式，请使用自动扩缩来主动管理表的吞吐能力或提前为表购买预留容量。切换到按需容量模式，以便按读取请求付费，仅为使用的容量付费。检测时间：6 天	ConsumedReadCapacityUnits

服务涵盖范围列表

对于某些服务， DevOpsGuru 会创建被动见解。被动见解可在异常行为发生时识别此类行为。它包含异常以及建议、相关指标和事件，可帮助您立即了解和解决问题。

对于某些服务，DevOpsGuru 会主动提供见解。主动见解可以让您在异常行为发生之前就了解它。它包含异常情况及建议，可帮助您在预测问题出现之前就将其解决。

DevOpsGuru 为以下服务创建被动见解：

- Amazon API Gateway
- Amazon CloudFront
- Amazon DynamoDB
- Amazon EC2

> **Note**
>
> DevOpsGuru 监控在 Auto Scaling 组级别进行，而不是在单个实例级别。

- Amazon ECS
- Amazon EKS
- AWS Elastic Beanstalk
- Elastic Load Balancing
- Amazon Kinesis
- AWS Lambda
- Amazon OpenSearch Service
- Amazon RDS
- Amazon Redshift
- Amazon Route 53
- Amazon S3
- Amazon SageMaker AI
- AWS Step Functions
- Amazon SNS
- Amazon SQS
- Amazon SWF
- Amazon VPC

DevOpsGuru 为以下服务提供主动见解：

- Amazon DynamoDB
- Amazon Kinesis
- AWS Lambda
- Amazon RDS
- Amazon SQS

设置 Amazon DevOps Guru

完成本节中的任务，首次设置 Amazon DevOps Guru。如果您已经有一个 AWS 账户，知道要分析哪个 AWS 或多个账户，并且有亚马逊简单通知服务主题可用于洞察通知，则可以直接跳到DevOpsGuru入门。

或者，您可以使用快速设置（一项功能）来设置 DevOps Guru 并快速配置其选项。 AWS Systems Manager您可以使用快速设置为独立账户或组织设置 DevOps Guru。要使用 Systems Manager 中的快速设置为组织设置 DevOps Guru，必须具备以下先决条件：

- 一个拥有 AWS Organizations. 有关更多信息，请参阅《AWS Organizations 用户指南》中的AWS Organizations术语和概念。
- 两个或多个组织单位 (OUs)。
- 每个 OU 中有一个或多个目标 AWS 账户。
- 一个具有管理目标账户权限的管理员账户。

要了解如何使用快速设置来设置 DevOps Guru，请参阅《AWS Systems Manager 用户指南》中的 “使用快速设置配置 DevOps Guru”。

使用以下步骤在不使用快速设置的情况下设置 DevOps Guru。

- 第 1 步 — 注册 AWS
- 第 2 步 — 确定 DevOps Guru 的覆盖范围
- 步骤 3 - 确定您的 Amazon SNS 通知主题

第 1 步 — 注册 AWS

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS 管理控制台在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in as the root user。
2. 为您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录 URL。

有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Add groups。

第 2 步 — 确定 DevOps Guru 的覆盖范围

您的边界覆盖范围决定了 Amazon DevOps Guru 对哪些 AWS 资源进行异常行为分析。我们建议您将资源分组到操作应用程序中。资源边界中的所有资源都应构成您的一个或多个应用程序。如果您有一个操作解决方案，那么您的覆盖范围应包括其所有资源。如果您有多个应用程序，请选择构成每个解决方案的资源，然后使用 CloudFormation 堆栈或 AWS 标签将它们分组在一起。您指定的所有组合资源，无论它们定义了一个还是多个应用程序，都将由 DevOps Guru 进行分析并构成其覆盖范围。

使用以下方法之一指定操作解决方案中的资源。

- 选择让您的 AWS 地区和账户定义您的覆盖范围。使用此选项， DevOps Guru 可以分析您账户和地区中的所有资源。如果您只将自己的账户用于一个应用程序，那么这是一个不错的选择。
- 使用 CloudFormation 堆栈来定义操作应用程序中的资源。 CloudFormation 模板为您定义和生成资源。在配置 DevOps Guru 时，请指定用于创建应用程序资源的堆栈。您可以随时更新堆栈。您选择的堆栈中的所有资源都定义了边界覆盖范围。有关更多信息，请参阅 使用 CloudFormation 堆栈来识别 DevOps Guru 应用程序中的资源。
- 使用 AWS 标签来指定应用程序中的 AWS 资源。 DevOpsGuru 仅分析包含您选择的标签的资源。这些资源构成了您的边界。

  AWS 标签由标签键和标签值组成。您可以指定一个标签键，也可以使用该键指定一个或多个值。对其中一个应用程序中的所有资源使用同一个值。如果您有多个应用程序，则对所有应用程序使用具有相同键的标签，并使用标签的值将资源分组到您的应用程序中。带有您选择的标签的所有资源构成了 DevOps Guru 的覆盖范围。有关更多信息，请参阅 使用标签来识别 DevOps Guru 应用程序中的资源。

如果您的边界覆盖范围包括构成多个应用程序的资源，则可以使用标签筛选您的见解，逐个应用程序查看见解。有关更多信息，请参阅查看 DevOps Guru 见解中的步骤 4。

有关更多信息，请参阅 使用 AWS 资源定义应用程序。有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。

步骤 3 - 确定您的 Amazon SNS 通知主题

您可以使用一两个 Amazon SNS 主题来生成有关重要的 DevOps Guru 事件的通知，例如何时创建见解。这样可以确保您尽快了解 DevOps Guru 发现的问题。设置 DevOps Guru 时，请准备好话题。使用 DevOps Guru 控制台设置 DevOps Guru 时，您可以使用通知主题的名称或其亚马逊资源名称 (ARN) 来指定通知主题。有关更多信息，请参阅启用 DevOps Guru。您可以使用 Amazon SNS 控制台查看每个主题的名称和 ARN。如果您没有主题，则可以在使用 Guru 控制台启用 DevOps Guru 时创建一个。 DevOps有关更多信息，请参阅《Amazon Simple Notification Service 开发人员指南》中的创建主题。

添加到 Amazon SNS 主题的权限

Amazon SNS 主题是一种包含 AWS Identity and Access Management (IAM) 资源策略的资源。当您在此处指定主题时， DevOpsGuru 会将以下权限附加到其资源策略中。

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

DevOpsGuru 需要这些权限才能使用主题发布通知。如果您不想拥有该主题的这些权限，则可以放心地将其删除，主题将继续按照您选择之前的方式运行。但是，如果删除了这些附加权限，DevOpsGuru 将无法使用该主题生成通知。

估算 Amazon DevOps Guru 资源分析成本

您可以估算 Amazon DevOps Guru 分析您的 AWS 资源的每月费用。您需要为指定资源涵盖范围内的每项活跃 AWS 资源所分析的小时数付费。仅当资源在一小时内生成指标、事件或日志时，该资源才处于活动状态。

DevOps Guru 会扫描您选择的资源以创建月度成本估算。您可以查看资源、其小时计费价格以及估算的每月费用。默认情况下，成本估算器假设已分析的活跃资源在 100% 的时间内都被利用。您可以根据估计使用量更改每项已分析服务的这一比例，以创建更新的每月成本估算。该估算值是分析您的资源的成本，不包括与 DevOps Guru API 调用相关的成本。

您一次可以创建一个成本估算。生成成本估算所需的时间取决于在创建成本估算时指定的资源数量。指定少量资源时，可能需要 1 到 2 个小时才能完成。指定大量资源时，可能需要多达 4 个小时才能完成。实际成本各不相同，取决于已分析活跃资源使用时间的比例。

> **Note**
>
> 对于成本估算，您只能指定一个 CloudFormation 堆栈。对于实际覆盖范围，最多可以指定 1000 个堆栈。

创建每月资源分析成本估算

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 在控制台导航窗格中，选择成本估算器。
3. 如果您尚未启用 DevOps Guru，则必须创建一个 IAM 角色。在出现的 “为 DevOps Guru 创建 IAM 角色” 弹出窗口中，选择同意创建 IAM 角色。这允许 DevOps Guru 在您选择开始成本估算分析或开始使用 DevOps Guru 时为您创建与 IAM 服务相关的角色。这样， DevOpsGuru 就拥有了创建成本估算所需的权限。如果您已经启用了 DevOps Guru，则该角色已经创建完毕，并且不会显示此选项。
4. 选择要用于创建估算值的资源。

   - 如果您想估计 DevOps Guru 分析由一个 CloudFormation 堆栈定义的资源的成本，请执行以下操作。

     1. 在当前区域中选择CloudFormation 堆栈。

2. 在选择堆 CloudFormation 栈中，选择您 AWS 账户中 CloudFormation 堆栈的名称。您也可以输入堆栈的名称以便快速找到它。有关使用和查看堆栈的信息，请参阅CloudFormation 用户指南中的使用堆栈。
3. （可选）如果您使用的 CloudFormation 堆栈当前未进行分析，请选择 “启用资源分析”，让 DevOps Guru 能够开始分析其资源。如果您尚未启用 DevOps Guru 或者您已经在分析堆栈中的资源，则此选项不可用。

- 如果您想估计 DevOps Guru 使用标签分析资源的成本，请执行以下操作。
  1. 在当前区域的 AWS 资源上选择标签
  2. 在标签键中，选择标签的键
  3. 在标签值中，选择（所有值）或选择一个值。
- 如果您想估算 DevOps Guru 分析您的 AWS 账户和区域中的资源的成本，请选择当前区域中的 AWS 账户。

5. 选择估算每月成本。
6. （可选）在活跃资源利用率 %列中，输入一项或多项 AWS 服务的更新百分比值。默认的活动资源利用率 %为 100%。这意味着， DevOps Guru 通过计算一小时分析其资源的成本，然后推断出 30 天总计 720 小时的成本，从而得出 AWS 服务的估算值。如果某项服务的活跃时间少于 100%，则可以根据估计使用量更新百分比，以获得更准确的估算。例如，如果您将某个服务的活动资源利用率更新为 75%，则分析其资源的一小时成本按 (720 x 0.75) 小时或 540 小时推断。

如果您的估算值为零，那么您选择的资源可能不包括 DevOps Guru支持的资源。有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。

DevOpsGuru 入门

在本节中，您将学习如何开始使用 Amazon DevOps Guru，以便它可以分析您的应用程序的运营数据和指标以生成见解。

主题

- 步骤 1：设置
- 第 2 步：启用 DevOps Guru
- 第 3 步：指定您的 DevOps Guru 资源覆盖范围

步骤 1：设置

在开始之前，请按照 设置 Amazon DevOps Guru 中的步骤进行准备。

第 2 步：启用 DevOps Guru

要将 Amazon DevOps Guru 配置为首次使用，您必须选择设置 DevOps Guru 的方式。您可以监控组织中的应用程序，也可以监控当前账户中的应用程序。

您可以监控整个组织的应用程序，也可以仅为往来账户启用 DevOps Guru。以下过程概述了根据您的需求设置 DevOps Guru的不同方法。

监控整个组织的账户

如果您选择监控整个组织的应用程序，请登录您的组织管理账户。您可以选择将组织成员账户设置为委托管理员。您一次只能有一个委托管理员，并且可以稍后修改管理员设置。管理账户和您设置的委托管理员账户均有权访问组织中所有账户的所有见解。

您可以使用控制台为您的组织添加跨账户支持，也可以使用 AWS CLI 来实现。

使用 DevOps Guru 控制台上线

您可以使用控制台为整个组织中的账户添加支持。

使用控制台让 DevOps Guru 能够查看汇总见解

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。

2. 选择 “监控组织中的应用程序” 作为设置类型。
3. 选择您想要用作被委派管理员的账户。选择 Register delegated administrator (注册委托管理员)。这样，任何启用了 DevOps Guru 的账户都可以访问整合视图。受委托的管理员可以整合查看您组织中的所有 DevOps Guru 见解和指标。您可以使用 SSM 快速设置功能或 AWS CloudFormation 堆栈集启用其他账户。要了解有关快速设置的更多信息，请参阅使用快速设置配置 DevOps Guru。要了解有关使用堆栈集进行设置的更多信息，请参阅CloudFormation 用户指南中的使用堆栈，以及 第 2 步 — 确定 DevOps Guru 的覆盖范围 和 使用 CloudFormation 堆栈来识别 DevOps Guru 应用程序中的资源。

使用 AWS CLI 上线

您可以使用 AWS CLI 让 DevOps Guru 查看聚合见解。运行以下命令。

```
aws iam create-service-linked-role --aws-service-name devops-guru.amazonaws.com --
description "My service-linked role to support DevOps Guru"

aws organizations enable-aws-service-access --service-principal devops-
guru.amazonaws.com

aws organizations register-delegated-administrator --account-id >ACCOUNT_ID< --service-
principal devops-guru.amazonaws.com
```

下表列出了指标。

命令	说明
`create-service-linked-role`	授予 DevOps Guru 收集有关您组织的信息的权限。如果此步骤不成功，请不要继续。
`enable-aws-service-access`	让你的组织加入 DevOps Guru。
`register-delegated-administrator`	允许访问成员账户以查看见解。

监控您的当前账户

如果您选择监控当前 AWS 账户中的应用程序，请选择覆盖或分析您的账户和区域中的哪些 AWS 资源，并指定一两个用于在创建见解时通知您的亚马逊简单通知服务主题。您可稍后根据需要更新这些设置。

启用 DevOps Guru 监控您当前 AWS 账户中的应用程序

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 选择监控当前 AWS 账户中的应用程序作为设置类型。
3. 在 DevOpsGuru 分析报道中，选择以下选项之一。

   - 分析当前 AWS 账户中的所有 AWS 资源： DevOpsGuru 会分析您账户中的所有 AWS 资源。
   - 选择稍后分析的 AWS 资源：您可以稍后选择分析边界。有关更多信息，请参阅确定 DevOps Guru 的覆盖范围和在 DevOps Guru 中更新你的 AWS 分析覆盖范围。

   DevOpsGuru 可以分析与其支持的 AWS 账户关联的任何资源。有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。
4. 您最多可以添加两个主题。 DevOpsGuru 使用一个或多个主题来通知你重要的 DevOps Guru 事件，例如创造新的见解。如果您现在没有指定主题，则可以稍后通过在导航窗格中选择 “设置” 来添加一个主题。

   a. 在指定 Amazon SNS 主题中，选择要使用的主题。

   b. 如要添加 Amazon SNS 主题，请执行以下操作之一。

      - 选择使用电子邮件生成新的 SNS 主题。然后，在指定电子邮箱地址中，输入要接收通知的电子邮箱地址。要输入其他电子邮箱地址，请选择添加新的电子邮箱。
      - 选择使用现有 SNS 主题。然后，从 “选择 AWS 账户中的主题” 中，选择要使用的主题。
      - 选择使用现有 SNS 主题 ARN 来指定来自另一账户的现有主题。然后，在输入主题的 ARN 中，输入主题 ARN。ARN 是主题的 Amazon 资源名称。您可以在不同的账户中指定主题。如果使用另一个账户中的主题，则必须向该主题添加资源策略。有关更多信息，请参阅 Amazon SNS 主题的权限。
5. 请选择启用。

要将 Amazon DevOps Guru 配置为首次使用，您必须选择覆盖或分析您的账户和区域中的哪些 AWS 资源，并指定一两个用于在创建见解时通知您的亚马逊简单通知服务主题。您可稍后根据需要更新这些设置。

第 3 步：指定您的 DevOps Guru 资源覆盖范围

如果您选择稍后在启用 DevOps Guru 时指定 AWS 资源，则需要在 AWS 账户中选择用于创建要分析的资源的 CloudFormation 堆栈。 CloudFormation 堆栈是您作为一个单元管理的 AWS 资源集合。您可以使用一个或多个堆栈来包含运行操作应用程序所需的所有资源，然后指定这些资源以便 DevOps Guru 对其进行分析。如果您未指定堆栈， DevOpsGuru 会分析您账户中的所有 AWS 资源。相关详情，请参阅CloudFormation 用户指南中的使用堆栈，以及 确定 DevOps Guru 的覆盖范围 和 使用 CloudFormation 堆栈来识别 DevOps Guru 应用程序中的资源。

> **Note**
>
> 有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。

指定 DevOps Guru 的资源覆盖范围

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 在导航窗格中，选择设置。
3. 在分析的资源中，选择编辑分析的资源。
4. 选择以下覆盖选项之一。

   - 如果您希望 DevOps Guru 分析您的账户和地区中所有支持的资源，请选择所有 AWS 账户资源。如果您选择此选项，则您的 AWS 账户就是您的资源分析覆盖范围。账户中每个堆栈中的所有资源都分组到各自的应用程序中。任何不在堆栈中的剩余资源都将分组到各自的应用程序中。
   - 如果您希望 DevOps Guru 分析您选择的CloudFormation 堆栈中的资源，请选择堆栈，然后选择以下选项之一。
     - 所有资源 — 分析您账户中堆栈中的所有资源。每个堆栈中的资源都分组到各自的应用程序中。系统不会分析账户中不在堆栈中的任何资源。
     - 选择堆栈 — 选择您希望 DevOps Guru 分析的堆栈。所选每个堆栈中的资源将分组到各自的应用程序中。您可以在查找堆栈中输入堆栈的名称以快速找到特定堆栈。您最多可以选择 1,000 个堆栈。

     有关更多信息，请参阅 使用 CloudFormation 堆栈来识别 DevOps Guru 应用程序中的资源。

- 如果您希望 DevOps Guru 分析包含您选择的标签的所有资源，请选择 “标签”。选择密钥，然后选择以下选项之一。
  - 所有账户资源 — 分析当前区域和账户中的所有 AWS 资源。具有所选标签键的资源按标签值（若有）进行分组。没有此标签键的资源将单独进行分组和分析。
  - 选择特定的标签值-将分析所有包含带有您选择的密钥的标签的资源。 DevOpsGuru 根据标签的值将您的资源分组到应用程序中。

  有关更多信息，请参阅 使用标签来识别 DevOps Guru 应用程序中的资源。
- 如果您不希望 DevOps Guru 分析任何资源，请选择 “无”。此选项禁用 DevOps Guru，这样您就可以停止因资源分析而产生费用。

5. 选择保存。

为 DevOps Guru 分析启用 AWS 服务

Amazon DevOps Guru 可以分析其支持的任何 AWS 资源的性能。当它发现异常行为时，它会生成一个见解，其中包含有关该行为及其解决方法的详细信息。有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。

DevOpsGuru 使用 Amazon CloudWatch 指标、 AWS CloudTrail 事件等来帮助分析资源。它支持的大多数资源都会自动生成 DevOps Guru 分析所需的指标。但是，一些 AWS 服务需要额外的操作才能生成所需的指标。对于某些服务，启用这些指标可以对现有的 DevOps Guru 覆盖范围进行额外分析。对于其他人来说，只有启用这些指标后才能进行分析。有关更多信息，请参阅确定 DevOps Guru 的覆盖范围 和在 DevOps Guru 中更新你的 AWS 分析覆盖范围。

需要采取行动才能进行 DevOps Guru 分析的服务

- Amazon 弹性容器服务 — 要生成其他指标来改善 DevOps Guru 对其资源的覆盖范围，请按照在 Amazon ECS 上设置容器见解中的步骤进行操作。这样做可能会产生亚马逊的 CloudWatch费用。
- Amazon Elastic Kubernetes Service — 要生成指标 DevOps供大师分析，请按照在亚马逊 EKS 和 Kubernetes 上设置容器见解中的步骤进行操作。 DevOps在设置这些指标的生成之前，Guru 不会分析任何 Amazon EKS 资源。这样做可能会产生亚马逊的 CloudWatch 费用。
- Amazon 简单存储服务 — 要生成指标供 DevOps Guru 分析，您必须启用请求指标。按照为存储桶中的所有对象创建 CloudWatch 指标配置中的步骤进行操作。 DevOps 在设置了这些指标的生成之前，Guru 不会分析任何 Amazon S3 资源。这样做可能会产生 CloudWatch 和 Amazon S3 的费用。

有关更多信息，请参阅 Amazon CloudWatch 定价。

在 DevOps Guru 中使用见解

当 Amazon DevOps Guru 检测到您的操作应用程序中的异常行为时，它会生成见解。 DevOpsGuru 会分析您在设置 DevOps Guru 时指定的 AWS 资源中的指标、事件等。每项见解都包含一项或多项建议，可用来缓解问题。它还包含指标列表、日志组列表以及用于识别异常行为的事件列表。

见解有两种类型。

- 被动见解提供可以用来解决当前正在发生的问题的建议。
- 积极的见解可以提供建议，以解决 DevOps Guru预测将来会发生的问题。

主题

- 查看 DevOps Guru 见解
- 在 DevOps Guru 控制台中了解见解
- 了解异常行为如何分组为见解
- 了解见解严重性

查看 DevOps Guru 见解

您可以使用查看您的见解 AWS 管理控制台。

查看您的 DevOps Guru 见解

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 打开导航窗格，然后选择 Cost Insights。
3. 在被动选项卡上，您可以看到被动见解的列表。在主动选项卡上，您可以看到主动见解的列表。
4. （可选）使用以下一个或多个筛选条件来查找您要寻找的见解。
   - 根据要查找的见解类型，选择被动或主动选项卡。
   - 选择筛选见解，然后选择一个选项来指定一个筛选器。您可以添加状态、严重性、资源和标签筛选器的组合。使用 AWS 标签筛选器仅查看由具有特定标签的资源生成的见解。要了解更多信息，请参阅使用标签来识别 DevOps Guru 应用程序中的资源。

> **Note**
>
> DevOpsGuru 可以分析以下资源，但无法使用标签筛选其见解。
>
> - Amazon API Gateway 路径和路由
> - Amazon DynamoDB Streams
> - Amazon EC2 Auto Scaling 组实例
> - AWS Elastic Beanstalk 环境
> - Amazon Redshift 节点

- 选择或指定要按见解创建时间进行筛选的时间范围。
  - 12h 显示过去 12 小时创建的见解。
  - 1d 显示过去一天创建的见解。
  - 1w 显示过去一周创建的见解。
  - 1m 显示过去一个月创建的见解。
  - 自定义允许您指定其他时间范围。可用于筛选见解的最大时间范围为 180 天。

5. 要查看见解的详细信息，请选择其名称。

在 DevOps Guru 控制台中了解见解

使用 Amazon DevOps Guru 控制台查看见解中的有用信息，以帮助您诊断和解决异常行为。当 DevOps Guru 分析您的资源并找到表明异常行为的相关 Amazon CloudWatch 指标、 AWS CloudTrail 事件和操作数据时，它会生成一个见解，其中包含解决问题的建议以及有关相关指标和事件的信息。使用洞察数据DevOpsGuru 最佳实践来解决 DevOps Guru 检测到的操作问题。

要查看见解，请按照查看见解中的步骤查找见解，然后选择其名称。见解页面包括以下详细信息。

见解概述

使用本节可获得对见解的高层次概述。您可以查看洞察的状态（持续或已关闭）、受影响的 CloudFormation 堆栈数量、洞察的开始、结束和上次更新的时间，以及相关的操作项（如果有）。

如果在堆栈级别对见解进行分组，则可以选择受影响的堆栈数量来查看其名称。产生见解的异常行为出现在受影响堆栈创建的资源中。如果在账户级别对见解进行分组，则数量为零或不显示。

有关更多信息，请参阅 了解异常行为如何分组为见解。

见解名称

见解的名称取决于它是按堆栈级别还是按账户级别分组的。

- 堆栈级别的见解名称包括包含具有异常行为的资源的堆栈的名称。
- 账户级别的见解名称不包含堆栈名称。

有关更多信息，请参阅 了解异常行为如何分组为见解。

聚合指标

选择聚合指标选项卡以查看与见解相关的指标。在表格中，每行代表一个指标。您可以看到哪个 CloudFormation 堆栈创建了发出该指标的资源、资源的名称及其类型。并非所有指标都与 CloudFormation 堆栈相关联或有名称。

当同时存在多个异常资源时，时间轴视图会聚合资源并在单个时间轴中显示其异常指标，以便于分析。时间轴上的红线表示指标发出异常值的时间跨度。要放大，请使用鼠标选择特定的时间范围。也可以使用放大镜图标放大和缩小。

选择时间轴中的一条红线以查看详细信息。在打开的窗口中，您可以：

- 选择查看范围 CloudWatch以查看该指标在 CloudWatch 控制台中的显示效果。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的统计数据和维度。
- 将鼠标悬停在图表上方可查看有关异常指标数据及其出现时间的详细信息。
- 选择带有向下箭头的方框可下载图表的 PNG 图像。

图表化异常

选择图表化异常选项卡可查看每个见解异常的详细图表。每个异常都会显示一个图块，其中包含相关指标中检测到的异常行为的详细信息。您可以在资源级别和每个统计数据中调查和查看异常。图表按指标名称进行分组。在每个图块中，您可以选择时间轴中的特定时间范围进行缩放。您也可以使用放大镜图标进行放大和缩小，或者选择以小时、天或周为单位的预定义持续时间（1H、3H、12H、1D、3D、1W 或 2W）。

选择查看所有统计数据和维度以查看有关异常的详细信息。在打开的窗口中，您可以：

- 选择查看范围 CloudWatch以查看该指标在 CloudWatch 控制台中的显示效果。
- 将鼠标悬停在图表上方可查看有关异常指标数据及其出现时间的详细信息。
- 选择统计数据或维度以自定义图表的显示方式。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的统计数据和维度。

日志组

启用日志异常检测后， DevOpsGuru 会标记您的 CloudWatch 日志组，以便您可以查看与您的见解相关的日志组。在见解详情页面的日志组部分，表中的每一行代表一个日志组并列出了相关资源。

当同时存在多个异常日志组时，时间轴视图会将它们聚合在单个时间轴中，以便于分析。时间轴上的紫线表示日志组遇到日志异常的时间跨度。

在时间轴中选择一条紫线可查看日志异常信息示例，例如关键字异常和数值偏差。选择查看日志组详细信息以查看日志异常。在打开的窗口中，您可以：

- 查看日志异常和相关事件的图表。
- 将鼠标悬停在图表上可查看有关异常日志数据及其发生时间的详细信息。
- 详细地查看日志异常，包括示例消息、出现频率、相关建议和出现时间。
- 单击 “查看详细信息” CloudWatch，查看异常日志中的日志行。

相关事件

在 “相关 AWS CloudTrail 事件” 中，查看与您的见解相关的事件。使用这些事件来帮助了解、诊断和解决异常行为的根本原因。

建议

在建议中，可以查看可能有助于您解决潜在问题的建议。当 DevOps Guru 检测到异常行为时，它会尝试创建推荐。见解可能包含一个、多个或零个建议。

了解异常行为如何分组为见解

见解按堆栈级别或账户级别进行分组。如果为 AWS CloudFormation 堆栈中的资源生成了见解，则它是堆栈级别的见解。否则，它是账户级别的见解。

堆栈的分组方式取决于您如何在 Amazon DevOps Guru 中配置资源分析范围。

如果涵盖范围是由 CloudFormation 堆栈定义的

将分析所选堆栈中包含的所有资源，并将所有检测到的见解按堆栈级别进行分组。

如果您的承保范围是您的往来 AWS 账户和地区

将分析您的账户和区域中的所有资源，检测到的见解有三种可能的分组方案。

- 从不属于堆栈的资源生成的见解按账户级别进行分组。
- 从处于前 10,000 个已分析堆栈的一个堆栈中的资源生成的见解按堆栈级别进行分组。

- 从一个不在前 10,000 个已分析堆栈的堆栈的资源生成的见解按账户级别进行分组。例如，为第 10,001 个已分析堆栈中的资源生成的见解按账户级别进行分组。

有关更多信息，请参阅 确定 DevOps Guru 的覆盖范围。

了解见解严重性

见解可以有三种严重性之一，即高、中或低。Amazon DevOps Guru 在检测到相关异常并为每个异常指定严重性后创建洞察。 DevOpsGuru 利用领域知识和多年的集体经验，将异常的严重性分为高、中或低。见解的严重性由导致创建见解的最严重异常决定。

- 如果生成见解的所有异常的严重性都为低，则该见解的严重性为低。
- 如果生成见解的所有异常的最高严重性为中，则该见解的严重性为中。产生见解的某些异常的严重性可能为低。
- 如果生成见解的所有异常的最高严重性为高，则该见解的严重性为高。产生见解的某些异常的严重程度可能为低或中。

使用 DevOps Guru 监控数据库

DevOpsGuru 为在上 AWS操作数据库提供了显著的价值。通过利用其机器学习算法， DevOpsGuru可以帮助优化数据库性能，提高可靠性并减少运营开销。用户指南的这一部分概述了这些数据库功能，包括不同 AWS 数据库服务的特定 DevOps Guru 用例。

DevOpsGuru 可以为诸如 Amazon RDS 之类的关系数据库提供见解。 Amazon Redshift它还可以为非关系数据库或 NoSQL 数据库（例如 Amazon DynamoDB 和）提供见解。 Amazon ElastiCache

主题

- 使用 DevOps Guru 监控关系数据库
- 使用 DevOps Guru 监控非关系数据库

使用 DevOps Guru 监控关系数据库

DevOpsGuru 从两个主要数据源中提取数据，在关系数据库中寻找见解和异常之处。对于 Amazon RDS 和 Amazon Redshift，将分析所有实例类型的 CloudWatch 销售指标。对于 Amazon RDS，还会提取以下引擎类型的 Performance Insights 数据：适用于 PostgreSQL 的 RDS、Aurora PostgreSQL 和 Aurora MySQL。

在 Amazon RDS 中监控数据库操作

本节包含有关在 DevOps Guru for RDS 中监控的用例和指标的具体信息，包括来自 CloudWatch 已售指标和 Performance Insights 的数据。有关 DevOps Guru for RDS 的更多信息，包括关键概念、配置和优势，请参阅the section called “在 DevOps Guru 中处理 RDS 中的异常情况”。

使用来自 CloudWatch 已售指标的数据监控 RDS

DevOpsGuru 能够通过提取默认 CloudWatch 指标（例如 CPU 利用率和读写操作延迟）来监控每种类型的 RDS 实例。由于这些指标是默认情况下出售的，因此当您使用 DevOps Guru 监控您的 RDS 实例时，无需进一步配置即可获得见解。 DevOpsGuru 会根据历史模式自动为这些指标建立基准，并将它们与实时数据进行比较，以检测数据库中的异常和潜在问题。

下表显示了从已 CloudWatch 售指标中获得的 Amazon RDS 潜在的被动见解列表。

AWS 由 DevOps Guru 监控的资源	DevOpsGuru 识别的场景	CloudWatch 监控的指标
Amazon RDS（所有实例类型）	CPU 或内存达到极限	DBLoad， DBLoadCPU
RDS for PostgreSQL	复制插槽延迟高	OldestReplicationSlotLag

DevOpsGuru 监控 CloudWatch 的来自 Amazon RDS 实例的其他销售指标：

- CPUUtilization
- DatabaseConnections
- DiskQueueDepth
- 失败了 SQLServer AgentJobsCount
- ReadLatency
- ReadThroughput
- ReplicaLag
- WriteLatency

使用 Performance Insights 中的数据监控

对于某些类型的 Amazon RDS 实例，例如 Aurora PostgreSQL、Aurora MySQL 和 PostgreSQL 版 RDS，您可以通过确保在这些实例上启用 Performance Insights 来解锁 Guru 监控的更多 DevOps功能。

DevOpsGuru 为各种情况提供反应式见解，包括以下场景：

DevOpsGuru 识别出来生成被动洞察力的场景
锁定争用问题
缺少索引
应用程序池配置错误
JDBC 默认值不理想

DevOpsGuru 为各种情况提供主动见解，包括以下场景：

AWS 由 DevOps Guru 监控的资源	DevOpsGuru 识别出来生成主动见解的场景
Aurora MySQL	InnoDB 历史列表变得过大，这可能会导致性能降低，例如数据库关闭时间过长
Aurora MySQL	在磁盘上创建的临时表数量增加，可能会影响数据库性能
适用于 PostgreSQL 的 RDS、Aurora PostgreSQL	在事务中闲置时间过长的连接、锁定锁定、阻塞其他查询以及阻止 vacum（包括自动真空）清理死行的潜在影响

监控中的数据库操作 Amazon Redshift

DevOpsGuru 能够通过提取默认 CloudWatch 指标（包括 CPU 利用率和已用磁盘空间的百分比）来监控您的 Amazon Redshift 资源。由于这些指标是默认出售的，因此 DevOps Guru 无需进一步配置即可自动监控您的 Amazon Redshift 资源。 DevOpsGuru 根据历史模式为这些指标建立基准，并将它们与实时数据进行比较以检测异常。

DevOpsGuru 识别的场景	CloudWatch 监控的指标
检测由集群工作负载、数据偏斜和未排序或领导节点任务等因素导致的 Amazon Redshift 实例 CPU 利用率过高	CPUUtilization
检测 Amazon Redshift 实例何时由于查询处理、分发和排序密钥、维护操作或墓碑块问题而耗尽磁盘空间	PercentageDiskSpaceUsed

来自 DevOps Guru 监控的 Amazon Redshift 实例的其他 CloudWatch 已售指标：

- DatabaseConnections
- HealthStatus
- MaintenanceMode

- NumExceededSchemaQuotas
- PercentageQuotaUsed
- QueryDuration
- QueryRuntimeBreakdown
- 读取 IOPS
- ReadLatency
- WLMQueue长度
- WLMQueueWaitTime
- WLMQuery持续时间
- WriteLatency

在 DevOps Guru 中处理 RDS 中的异常情况

DevOpsGuru 检测、分析支持的 AWS 资源（包括 Amazon RDS 引擎）并提供建议。对于启用了 Performance Insights 的 Amazon Aurora 和 RDS for PostgreSQL 数据库实例 DevOps，Guru for RDS 对性能问题进行了详细的、针对数据库的分析，并建议了纠正措施。

主题

- DevOpsRDS 版 Guru 概述
- 为 DevOps RDS 启用 Guru
- 分析 Amazon RDS 中的异常

DevOpsRDS 版 Guru 概述

下面，您可以找到 DevOps Guru for RDS 的主要优势和功能的摘要。有关见解和异常情况的背景信息，请参阅DevOps大师概念。

主题

- DevOpsGuru 为 RDS 带来的好处
- 数据库性能调整的主要概念
- 适用于 DevOps RDS 的 Guru 的关键概念
- RDS DevOps 版 Guru 的工作原理
- 支持的数据库引擎

DevOpsGuru 为 RDS 带来的好处

如果您对 Amazon RDS 数据库负责，则可能不知道正在发生影响该数据库的事件或回归。当您了解这个问题时，您可能不知道为什么会发生这个问题，也不知道该怎么处理它。您可以遵循 DevOps Guru for RDS 的建议，而不必向数据库管理员 (DBA) 寻求帮助或依赖第三方工具。

通过对 DevOps Guru for RDS 的详细分析，您可以获得以下优势：

快速诊断

DevOpsGuru for RDS 持续监控和分析数据库遥测数据。Performance Insights、增强监控和 Amazon 会为您的数据库实例 CloudWatch 收集遥测数据。 DevOpsGuru for RDS 使用统计和机器学习技术来挖掘这些数据并检测异常。要了解有关 Amazon Aurora 数据库的遥测数据的更多信息，请参阅《Amazon Aurora 用户指南》中的使用 Amazon Aurora 上的性能见解监控数据库负载和使用增强监控功能来监控操作系统。要了解有关其他 Amazon RDS 数据库的遥测数据的更多信息，请参阅《Amazon Aurora 用户指南》中的使用 Amazon 关系数据库服务上的性能见解监控数据库负载和使用增强监控功能来监控操作系统。

快速解决方案

每个异常情况都会识别性能问题，并建议调查或纠正措施的途径。例如， DevOpsGuru for RDS 可能会建议您调查特定的等待事件。或者，它可能建议您优化应用程序池设置以限制数据库连接的数量。根据这些建议，您可以比手动进行故障排除更快地解决性能问题。

主动见解

DevOpsGuru for RDS 使用您的资源中的指标来检测潜在的问题行为，以免其成为更大的问题。例如，它可以检测连接到数据库的会话何时未执行活动工作以及可能阻塞数据库资源。 DevOps 然后，Guru 会提供建议，帮助你在问题变成更大的问题之前解决问题。

深入了解 Amazon 工程师和机器学习

为了检测性能问题并帮助您解决瓶颈， DevOpsGuru for RDS 依靠机器学习 (ML) 和高级统计分析。Amazon 数据库工程师为 DevOps Guru for RDS 研究结果的开发做出了贡献，该发现概括了多年来管理数十万个数据库的经验。通过利用这些集体知识， DevOpsGuru for RDS 可以教你最佳实践。

数据库性能调整的主要概念

DevOpsGuru for RDS 假设你熟悉一些关键的性能概念。要了解有关这些概念的更多信息，请参阅《Amazon Aurora 用户指南》的性能见解概述或《Amazon RDS 用户指南》的性能见解概述。

主题

- 指标
- 问题检测
- 数据库加载
- 等待事件

指标

指标代表一个按时间顺序排列的数据点集。可将指标视为要监控的变量，而数据点代表该变量随时间变化的值。Amazon RDS 为数据库和 DB 实例所运行的操作系统 (OS) 实时提供指标。您可以在 Amazon RDS 控制台上查看 Amazon RDS 数据库实例的所有系统指标和流程信息。 DevOps Guru for RDS 可以监控其中一些指标并提供有关这些指标的见解。有关更多信息，请参阅在 Amazon Aurora 集群中监控指标或在 Amazon 关系数据库关系实例中监控指标 。

问题检测

DevOpsGuru for RDS 使用数据库和操作系统 (OS) 指标来检测关键的数据库性能问题，无论这些问题是即将发生的还是持续的。 DevOpsGuru for RDS 问题检测主要有两种工作方式：

- 使用阈值
- 使用异常

使用阈值检测问题

阈值是据以评估受监控指标的临界值。您可以将阈值视为指标图表上的一条水平线，用于区分正常行为和潜在有问题的行为。 DevOps Guru for RDS 可监控特定指标，并通过分析哪些级别被认为对特定资源有潜在问题来创建阈值。 DevOps然后，当新的指标值在给定时间段内持续超过指定阈值时，DevOpsGuru for RDS 会在 Guru 控制台中创建见解。这些见解包含防止将来影响数据库性能的建议。

例如， DevOpsGuru for RDS 可能会在 15 分钟内监控使用磁盘的临时表的数量，并在临时表每秒使用磁盘的速率异常高时创建见解。磁盘上临时表使用量增加可能会影响数据库性能。 DevOpsGuru for RDS 通过在情况变得危急之前将其暴露出来，可以帮助您采取纠正措施来防止出现问题。

检测异常问题

虽然阈值为检测数据库问题提供了一种简单而有效的方法，但这些在某些情况下还不够。考虑这样一种情况：由于已知流程（例如每日报告任务），指标值经常激增并演变为可能存在问题的行为。由于预计会出现这样的激增，因此为每个激增创建见解和通知会适得其反，并可能导致警报疲劳。

但是，仍然有必要检测非常不寻常的激增，因为比其他指标高得多或持续时间更长的指标可能代表真正的数据库性能问题。为了解决这个问题， DevOpsGuru for RDS 会监控某些指标，以检测指标的行为何时变得非常异常或异常。 DevOps然后，Guru 在见解中报告了这些异常情况。

例如， DevOpsGuru for RDS 可能会在数据库负载不仅很高而且与其通常行为明显偏离时创建见解，这表明数据库操作出现了意想不到的严重减速。通过仅识别异常的数据库负载峰值， DevOpsGuru for RDS 可让您专注于真正重要的问题。

数据库加载

数据库调整的主要概念是数据库负载（DB 负载）指标。数据库负载表示数据库在任何给定时间的繁忙程度。数据库负载增加意味着数据库活动增加。

数据库会话表示的是应用程序与关系数据库的对话。活动会话是指正在运行数据库请求的会话。当会话在 CPU 上运行或等待资源变为可用以便继续执行时，该会话即处于活动状态。例如，活动会话可能会等待页面被读入内存，然后占用 CPU 以从页面读取数据。

性能见解中的DBLoad指标可在平均活动会话 (AAS)中衡量。为了计算 AAS，“性能见解”会对每秒的活动会话数进行采样。平均活动会话数等于活动会话总数除以特定时间段内的样本总数。AAS 值为 2 表示平均而言，在任何指定时间内请求中有 2 个会话是活动的。

数据库负载可以类比成仓库中的活动。假设仓库雇用了 100 名工人。如果收到 1 个订单，则会有 1 名工人配送订单，而其他工人则继续闲置。如果收到 100 个或更多订单，则所有 100 名工人将同时完成订单。如果您定期在给定时间段内进行抽样，了解有多少工人处于活动状态，则可以计算活动工人的平均数量。计算表明，平均而言，在任何指定时间内都会有 N 名工人忙于配送订单。如果昨天平均为 50 名工人而今天为 75 名工人，那么仓库的活动水平就会提升。同样的，数据库负载会随着会话活动的增加而增加。

要了解更多信息，请参阅《Amazon Aurora 用户指南》中的数据库加载或《Amazon RDS 用户指南》中的数据库加载。

等待事件

等待事件是一种数据库工具类型，它告诉您数据库会话正在等待哪个资源，以便它可以继续。当“性能见解”计算活动会话以计算数据库负载时，它还会记录导致活动会话等待的等待事件。该技术让“性能见解”可以向您显示哪些等待事件导致了数据库负载。

每个活动的会话要么会在 CPU 上运行，要么仍在等待。例如，在搜索内存、执行计算或运行过程代码时，会话都会占用 CPU。当会话不占用 CPU 时，它们可能正在等待要读取的数据文件或等待将要写入的日志。会话等待资源的时间越长，它在 CPU 上运行的时间就越少。

当您优化数据库时，经常尝试找出会话正在等待的资源。例如，两三个等待事件可能会占据数据库负载的 90% 这一测量结果表明，平均而言，活动会话花费了大部分时间用于等待少量资源。如果您能找出导致这些等待的原因，就可以尝试纠正问题。

想想仓库工人的类比。收到了一个订单，内容是一本书。工人在配送订单时可能会出现延迟。例如，其他的工人目前可能正在补货架，因此手推车可能已被占用。或者用于输入订单状态的系统可能运行缓慢。工人等待的时间越长，完成订单所需的时间就越长。等待是仓库工作流程中常见的现象，但是如果等待时间过长，生产力就会降低。同样，重复或冗长的会话等待可能会降低数据库性能。

有关 Amazon Aurora 中等待事件的更多信息，请参阅《Amazon Aurora 用户指南》中的为 Aurora PostgreSQL 优化等待事件和为 Aurora MySQL 优化等待事件。

有关其他 Amazon RDS 数据库中的等待事件的更多信息，请参阅《Amazon RDS 用户指南》中的使用 RDS for PostgreSQL 的等待事件进行调整。

适用于 DevOps RDS 的 Guru 的关键概念

DevOpsGuru 在您的操作应用程序中检测到异常或有问题的行为时，就会生成见解。见解包含一个或多个资源的异常。异常表示 DevOps Guru 检测到的一个或多个意外或异常的相关指标。

见解的严重性分为高、中或低。见解的严重性由促成该见解的最严重异常所决定。例如，如果洞察 AWS-ECS_ MemoryUtilization _and_others 包含一个严重性较低的异常和另一个严重性较高的异常，则该洞察的总体严重性为高。

如果 Amazon RDS 数据库实例启用了 Performance Insights，则 DevOps Guru for RDS 会针对这些实例的异常情况提供详细的分析和建议。为了识别异常情况， DevOpsGuru for RDS 为数据库指标值制定了基准。 DevOps然后，Guru for RDS 将当前指标值与历史基线进行比较。

主题

- 主动见解
- 被动见解
- 建议

主动见解

主动见解可以让您在问题发生之前了解问题行为。它包含异常情况以及建议和相关指标，可以帮助您解决问题，以免问题变得更严重。

每个主动见解页面都提供有关一个异常的详细信息。

被动见解

被动见解可在异常行为发生时识别此类行为。它包含异常以及建议、相关指标和事件，可帮助您立即了解和解决问题。

因果异常

因果异常是被动见解内的一项顶级异常。它在 DevOps Guru 控制台的异常详细信息页面上显示为主要指标。 数据库负载（数据库负载）是 DevOps Guru for RDS 的因果异常。例如，见解 AWS-ECS_MemoryUtilization _and_ot hers 可能有多个指标异常，其中一个是资源 AWS/RDS 的数据库负载（数据库负载）。

在见解中，多个 Amazon RDS 数据库实例可能会出现异常数据库负载（DB 负载）。异常的严重性对每个数据库实例都可能不同。例如，一个数据库实例的严重性可能为高，而其他数据库实例的严重性可能为低。控制台默认为严重性最高的异常。

上下文异常

上下文异常是数据库负载（DB 负载）内与被动见解相关的一项调查结果。它显示在 DevOps Guru 控制台异常详情页面的相关指标部分中。每个上下文异常都描述了需要调查的特定 Amazon RDS 性能问题。例如，因果异常可能包括以下上下文异常：

- 超出 CPU 容量 — CPU 运行队列或 CPU 利用率高于正常水平。
- 数据库内存不足 — 进程没有足够的内存。
- 数据库连接峰值 – 数据库连接数量超过正常值。

建议

每个见解至少有一个建议的操作。以下示例是 DevOps Guru 为 RDS 生成的建议：

- 调整 SQL IDs *`list_of_IDs`* 以降低 CPU 使用率，或者升级实例类型以增加 CPU 容量。
- 查看当前数据库连接的相关峰值。考虑调整应用程序池设置，以避免频繁地动态分配新的数据库连接。
- 查找执行过多内存操作（例如内存中排序或大型连接）的 SQL 语句。
- 调查以下 SQL 的大 I/O 量使用情况 IDs:*`list_of_IDs`*.
- 检查是否存在创建大量临时数据的语句，例如那些执行大量排序或使用大型临时表的语句。
- 检查应用程序以了解导致数据库工作负载增加的原因。

- 考虑启用 MySQL 性能架构。
- 检查是否存在长时间运行的事务，然后以提交或回滚将其结束。
- 配置 idle_in_transaction_session_timeout 参数，以结束处于“空闲事务”状态超过指定时间的任何会话。

RDS DevOps 版 Guru 的工作原理

DevOpsGuru for RDS 收集指标数据并对其进行分析，然后在控制面板中发布异常情况。

主题

- 数据收集和分析
- 异常发布

数据收集和分析

DevOpsGuru for RDS 从 Amazon RDS Performance Insights 收集有关您的亚马逊 RDS 数据库的数据。此功能可监控 Amazon RDS 数据库实例，收集指标，并让您能够浏览图表中的指标。最重要的性能指标是DBLoad。 DevOpsGuru for RDS 使用 Performance Insights 指标并对其进行分析以检测异常。有关“性能见解”的更多信息，请参阅《Amazon Aurora用户指南》中的使用 Amazon Aurora 上的性能见解监控数据库负载或《Amazon RDS 用户指南》中的使用 Amazon RDS 上的性能见解监控数据库负载。

DevOpsGuru for RDS 使用机器学习和高级统计分析来分析其从 Performance Insights 收集的数据。如果 DevOps Guru for RDS 发现性能问题，则会继续执行下一步。

异常发布

数据库性能问题（例如数据库负载高）可能会降低数据库的服务质量。当 DevOps Guru 在 RDS 数据库中检测到问题时，它会在控制面板中发布见解。该见解包含资源 AWS/RDS 的异常。

如果您的实例启用了 Performance Insights，则异常会包含对问题的详细分析。 DevOps Guru for RDS 还建议您进行调查或采取特定的纠正措施。例如，建议可能是调查特定的高负载 SQL 语句，考虑增加 CPU 容量或关闭 idle-in-transaction会话。

支持的数据库引擎

DevOps以下数据库引擎支持 Guru for RDS：

与 MySQL 兼容的 Amazon Aurora

有了解此引擎的更多信息，请参阅《Amazon Aurora 用户指南》中的使用 Amazon Aurora MySQL。

与 PostgreSQL 兼容的 Amazon Aurora

要了解有关此引擎的更多信息，请参阅《Amazon Aurora 用户指南》中的使用 Amazon Aurora PostgreSQL。

Amazon RDS for PostgreSQL 兼容性

要了解有关此引擎的更多信息，请参阅《Amazon RDS 用户指南》中的Amazon RDS for PostgreSQL。

DevOpsGuru 报告异常情况，并对其他数据库引擎进行基本分析。 DevOpsGuru for RDS 仅为 Amazon Aurora 和 RDS for PostgreSQL 实例提供详细的分析和建议。

为 DevOps RDS 启用 Guru

当您启用 DevOps Guru for RDS 时， DevOpsGuru 可以分析数据库实例等资源中的异常情况。Amazon RDS 使得可以轻松地发现 RDS 数据库实例或数据库集群并启用建议的功能。为了实现这一目标，RDS 会对其他服务（例如 Amazon EC2、 DevOps Guru 和 IAM）进行 API 调用。当 RDS 控制台进行这些 API 调用时，会将其 AWS CloudTrail 记录下来以供查看。

要允许 DevOps Guru 发布有关 Amazon RDS 数据库的见解，请完成以下各节中的任务。

主题

- 为您的 Amazon RDS 数据库实例开启“性能见解”
- 为 DevOps Guru for RDS 配置访问策略
- 将 Amazon RDS 数据库实例添加到您的 DevOps Guru 覆盖范围中

为您的 Amazon RDS 数据库实例开启“性能见解”

要让 DevOps Guru for RDS 分析数据库实例上的异常，请确保已开启 Performance Insights。如果数据库实例未开启 Performance Insigh DevOps ts，则 Guru for RDS 会在以下位置通知您：

控制面板

如果按资源类型查看见解，RDS 图块会提醒“性能见解”未开启。选择此链接以在 Amazon RDS 控制台开启“性能见解”。

见解

在页面底部的推荐部分，选择启用 Amazon RDS 性能见解。

设置

在服务：Amazon RDS 部分，选择此链接以在 Amazon RDS 控制台开启“性能见解”。

有关更多信息，请参阅《Amazon Aurora 用户指南》中的开启和关闭性能见解，或《Amazon RDS 用户指南》中的开启和关闭性能见解。

为 DevOps Guru for RDS 配置访问策略

要让用户访问 DevOps Guru for RDS，他们必须拥有以下任一策略的权限：

- AWS 托管策略 `AmazonRDSFullAccess`
- 允许执行以下操作的客户托管策略：
  - `pi:GetResourceMetrics`
  - `pi:DescribeDimensionKeys`
  - `pi:GetDimensionKeyDetails`

有关更多信息，请参阅《Amazon Aurora 用户指南》中的配置性能见解的访问策略，或《Amazon RDS 用户指南》中的配置性能见解的访问策略。

将 Amazon RDS 数据库实例添加到您的 DevOps Guru 覆盖范围中

您可以在 DevOps Guru 控制台或 Amazon RDS 控制台中配置 DevOps Guru 来监控您的 Amazon RDS 数据库。

在 DevOps Guru 控制台中，您可以选择以下选项：

- 在账户级别开启 DevOps Guru。这是默认值。当您选择此选项时， DevOpsGuru 会分析您的 AWS 区域 和中所有支持的 AWS 资源 AWS 账户，包括 Amazon RDS 数据库。
- 为 DevOps RDS 的 Guru 指定 AWS CloudFormation 堆栈。

  有关更多信息，请参阅 使用 CloudFormation 堆栈来识别 DevOps Guru 应用程序中的资源。
- 标记 Amazon RDS 资源。

  标签是您分配给 AWS 资源的自定义属性标签。使用标签来标识构成应用程序的 AWS 资源。然后，您可以按标签筛选详情，以便只查看您的应用程序创建的见解。要仅查看应用程序中的 Amazon

RDS 资源生成的见解，请为 Amazon RDS 资源标签添加一个值，例如`Devops-guru-rds`。有关更多信息，请参阅 使用标签来识别 DevOps Guru 应用程序中的资源。

> **Note**
>
> 在为 Amazon RDS 资源添加标签时，必须为数据库实例而不是集群添加标签。

要从 Amazon RDS 控制台启用 DevOps Guru 监控，请参阅在 RDS 控制台中打开 DevOps Guru。请注意，要从 Amazon RDS 控制台启用 DevOps Guru，您必须使用标签。有关标签的更多信息，请参阅the section called “使用标签识别应用程序中的资源”。

分析 Amazon RDS 中的异常

当 DevOps Guru for RDS 在控制面板中发布性能异常时，您通常会执行以下步骤：

1. 在 DevOps Guru 仪表板中查看见解。 DevOpsGuru for RDS 报告了被动和主动见解。

   有关更多信息，请参阅 查看见解。
2. 查看 AWS/RDS 资源的异常。

   有关更多信息，请参阅查看被动异常和查看主动异常。
3. 回复 DevOps Guru 以获取 RDS 建议。

   有关更多信息，请参阅 响应建议。
4. 监控数据库实例的运行状况，确保已解决的性能问题不会再出现。

   有关更多信息，请参阅《Amazon Aurora 用户指南》中的监控 Amazon Aurora 数据库集群的指标和《Amazon RDS 用户指南》中的监控 Amazon RDS 实例的指标。

查看见解

访问 DevOps Guru 控制台中的 “见解” 页面，查找被动和主动见解。从那里，您可以从列表中选择一个见解，以查看详细的指标、建议以及有关该见解的更多信息。

查看一个见解

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 打开导航窗格，然后选择见解。

3. 选择被动选项卡查看被动见解，或选择主动查看主动见解。
4. 选择一个见解的名称，按状态和严重性排列优先级。

   将显示详细的见解页面。

查看被动异常

在见解中，您可以查看 Amazon RDS 资源的异常。在被动见解页面的聚合指标部分，可以查看带有相应时间线的异常列表。还有一些部分显示与异常相关的日志组和事件的信息。被动见解中的因果异常每个都有相应的页面，其中包含有关异常的详细信息。

查看对 RDS 被动异常的详细分析

在此阶段，深入研究该异常，以获取有关 Amazon RDS 数据库实例的详细分析和建议。

详细分析仅适用于开启了“性能见解”的 Amazon RDS 数据库实例。

深入研究异常详情页面

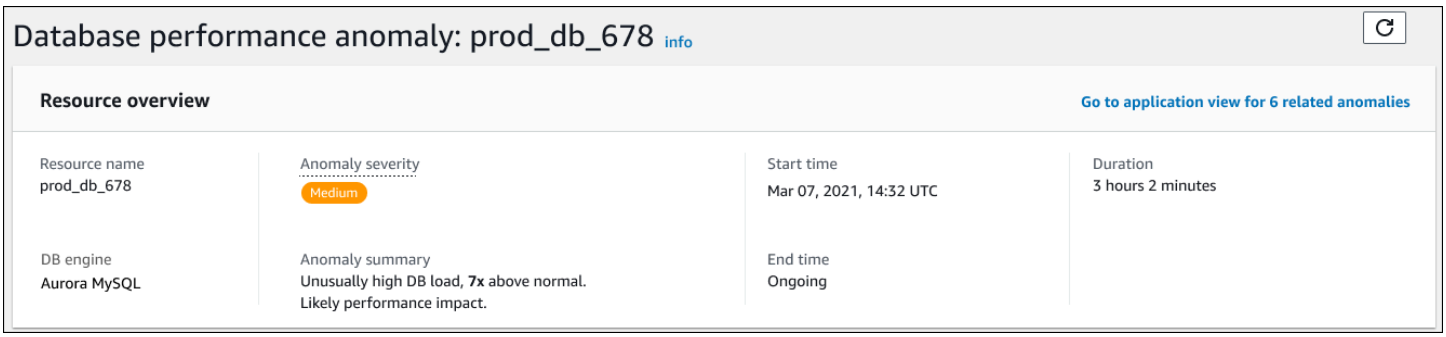
1. 在见解页面上，找到资源类型为 AWS/RDS 的聚合指标。
2. 请选择查看详细信息。

   出现异常详细信息页面。标题以数据库性能异常开头，并命名资源显示。无论异常何时出现，控制台都默认为严重性最高的异常。
3. （可选）如果多个资源受到影响，则从页面顶部的列表中选择一个不同的资源。

随后您可以找到对详情页面构成部分的说明。

资源概述

详情页面的顶部是资源概述。此部分总结了 Amazon RDS 数据库实例遇到的性能异常。

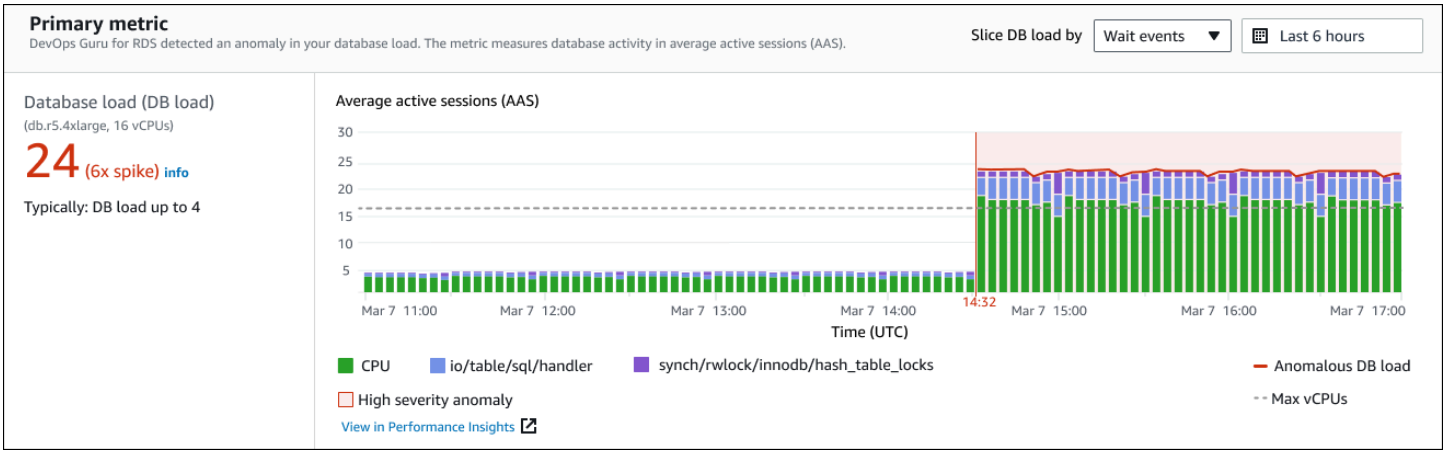


此部分包含以下字段：

- 资源名称 — 遇到异常的数据库实例的名称。在此示例中，该资源被命名为prod_db_678。
- 数据库引擎 — 遇到异常的数据库实例的名称。在此示例中，引擎是 Aurora MySQL。
- 异常严重性 — 衡量异常对实例的负面影响的标准。可能的严重性包括高、中和低。
- 异常摘要 — 对问题的简要综述。典型的摘要是数据库负载异常高。
- 开始时间和结束时间 — 异常开始和结束的时间。如果结束时间为持续，则异常仍在发生。
- 持续时间 — 异常行为的持续时间。在此示例中，异常持续存在，已经出现了 3 小时 2 分钟。

主要指标

主要指标部分汇总了因果异常，即见解中的最高一级异常。可以将因果异常视为数据库实例遇到的一般问题。



左侧面板提供了有关该问题的更多详细信息。在此示例中，摘要包含以下信息：

- 数据库负载（DB 负载）— 将异常归类为数据库负载问题。“性能见解”中的相应指标是DBLoad。该指标也已发布到亚马逊 CloudWatch。
- db.r5.4xlarge — 数据库实例类。v CPUs 的数量（在本例中为 16）对应于平均活跃会话数 (AAS) 图表中的虚线。
- 24（6 倍峰值）— 数据库负载，在见解报告的时间间隔内的平均活动会话 (AAS) 数量来衡量。因此，在异常期间的任何给定时间，数据库上平均有 24 个会话处于活动状态。数据库负载是该实例正常数据库负载的 6 倍。
- 典型：数据库负载最多为 4 — 典型工作负载期间以 AAS 衡量的数据库负载基准。值 4 表示，在正常操作期间，在任何给定时间，数据库上平均有 4 个或更少的会话处于活动状态。

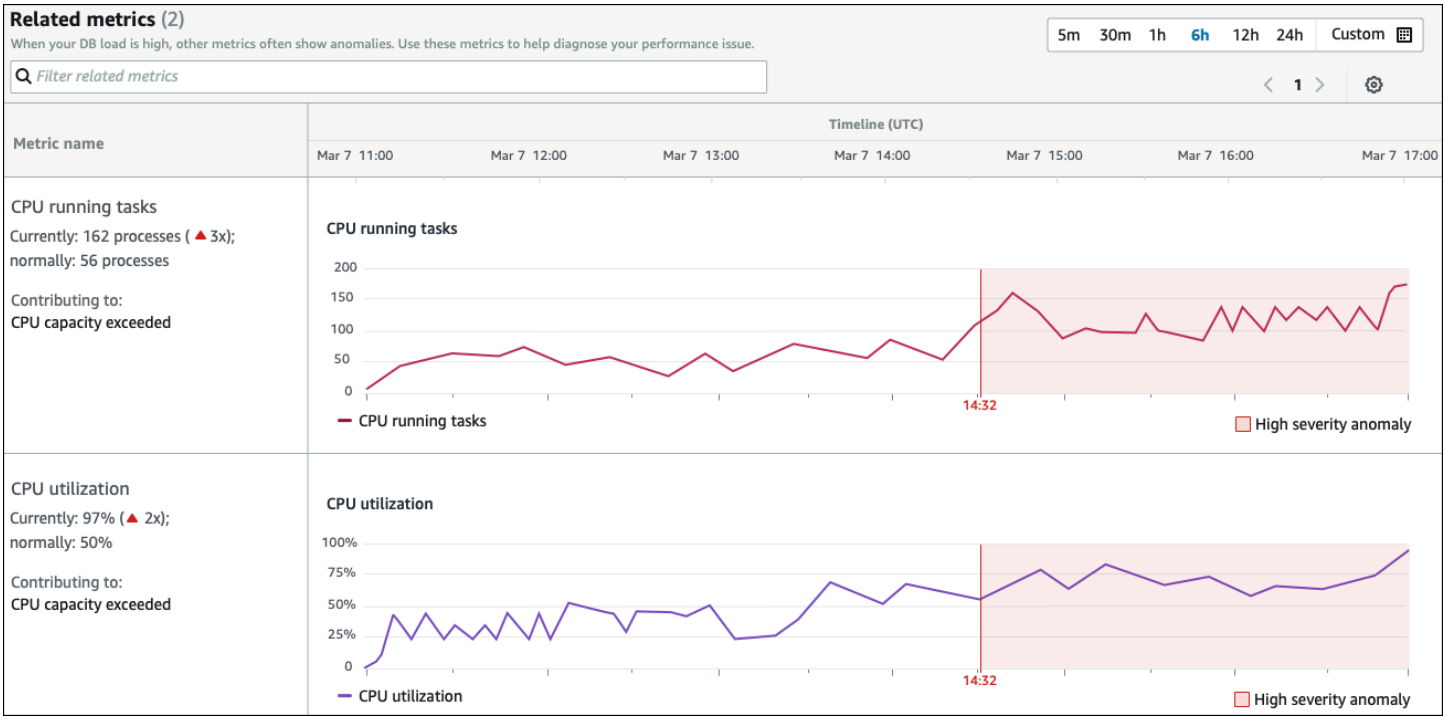
默认情况下，负载图表由等待事件进行切片。这意味着，对于图表中的每个条形，最大的彩色区域表示占数据库总负载最多的等待事件。图表显示了问题开始的时间（红色）。将注意力集中于在条形中占用空间最多的等待事件：

- CPU
- IO:wait/io/sql/table/handler

对于此 Aurora MySQL 数据库，上述等待事件出现的次数比正常情况要多。如需了解如何使用 Amazon Aurora 中的等待事件来调优性能，请参阅《Amazon Aurora 用户指南》中的为 Aurora MySQL 优化等待事件和为 Aurora PostgreSQL 优化等待事件。要了解如何在 RDS for PostgreSQL 中使用等待事件调整性能，请参阅《Amazon RDS 用户指南》中的使用 RDS for PostgreSQ 等待事件进行调整。

相关指标

相关指标部分列出了上下文异常，这些异常是因果异常中的具体发现。这些发现提供了有关性能问题的额外信息。



相关指标表有两列：指标名称和时间线 (UTC)。表中的每一行都对应特定的指标。

每行的第一列包含以下信息：

- ***Name***— 指标的名称。第一行将该指标标记为 CPU 运行任务。

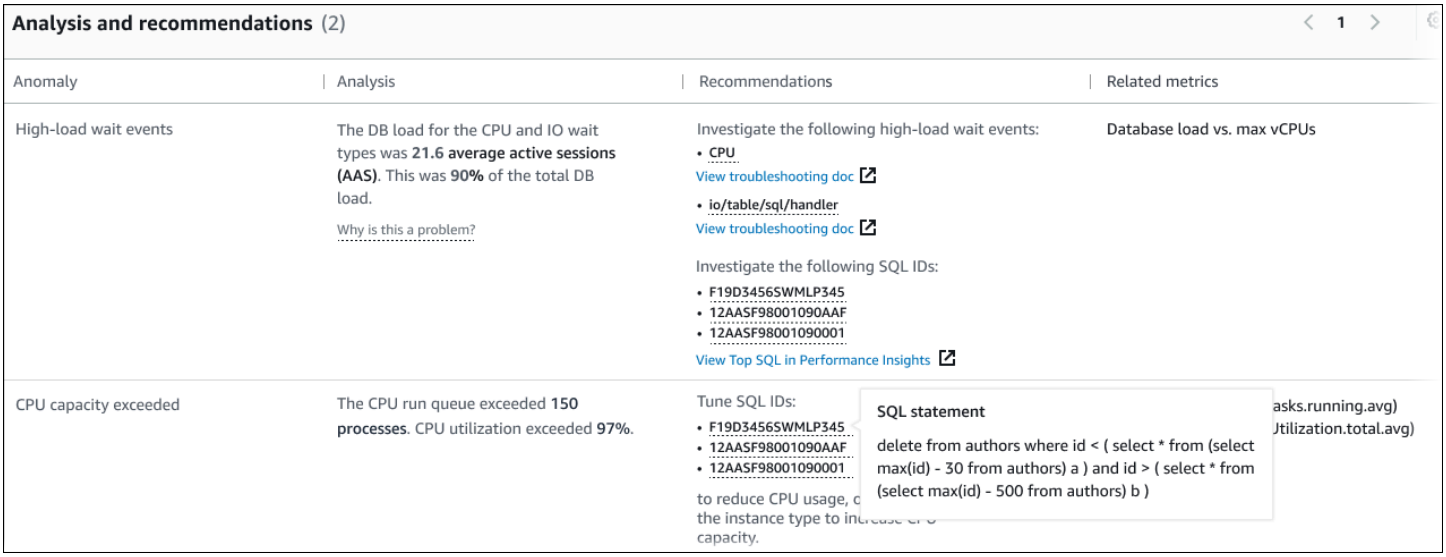
- 当前 — 指标的当前值。在第一行，当前值为 162 个进程 (3x)。
- 通常-此数据库正常运行时的该指标的基准。 DevOpsGuru for RDS 将基线计算为历史记录 1 周内的第 95 个百分位数值。第一行表示 CPU 上通常有 56 个进程在运行。
- 促成 — 与该指标相关的发现。在第一行，CPU 运行任务指标与 CPU 容量超出异常关联。

时间线列显示该指标的折线图。阴影区域显示了 DevOps Guru for RDS 将发现指定为高严重性的时间间隔。

分析和建议

因果异常描述了总体问题，而上下文异则描述了需要调查的特定发现。每个发现都对应一组相关指标。

在以下分析和建议部分的示例中，高数据库负载异常有两个发现。



此表包含以下各列：

- 异常 — 对此上下文异常的一般描述。在此示例中，第一个异常是高负载等待事件，第二个异常是超出 CPU 容量。
- 分析 — 对异常的详细解释。

  在第一个异常中，三种等待类型占数据库负载的 90%。在第二个异常中，CPU 运行队列超过 150，这意味着在任何给定时间，有超过 150 个会话在等待 CPU 时间。CPU 利用率超过 97%，这意味着在问题持续期间，CPU 有 97% 的时间处于忙碌状态。因此，CPU 几乎持续被占用，而平均有 150 个会话等待在 CPU 上运行。
- 建议 — 建议的用户对异常的响应。

在第一个异常中， DevOpsGuru for RDS 建议您调查等待事件cpu和。io/table/sql/handler要了解如何根据这些事件调整数据库性能，请参阅 cpu 和 io/table/sql/handlerAmazon Aurora 用户指南。

在第二个异常情况中， DevOpsGuru for RDS 建议您通过调整三个 SQL 语句来降低 CPU 消耗。您可以将鼠标悬停在链接上方以查看 SQL 文本。

- 相关指标 — 提供对异常进行具体衡量的指标。有关这些指标的更多信息，请参阅《Amazon Aurora 用户指南》中的 Amazon Aurora 指标参考或《Amazon RDS 用户指南》中的 Amazon RDS 指标参考。

  在第一个异常中， DevOpsGuru for RDS 建议将数据库负载与实例的最大 CPU 进行比较。在第二个异常中，建议查看 CPU 运行队列、CPU 利用率和 SQL 执行率。

查看主动异常

在见解中，可以查看 Amazon RDS 资源的异常。每个主动见解都提供有关一个主动异常的详细信息。在主动见解页面上，可以查看见解概述、有关异常的详细指标以及防止将来出现问题的建议。要查看主动异常，请转到主动见解页面。

见解概述

见解概述部分详细介绍了创建见解的原因。它显示了见解的严重性、异常的描述和异常发生的时间范围。它还列出了 DevOps Guru 检测到的受影响服务和应用程序的数量。

指标

指标部分提供了关于异常的图表。每个图表都显示由资源的基线行为确定的阈值，以及从异常发生时起报告的指标数据。

聚合资源建议

此部分提供了可以采取哪些措施来缓解所报告问题以免它们成为更大问题的建议。可以采取的操作显示在建议的自定义更改列中。这些建议背后的理由在《 DevOps Guru 为什么要推荐这个？》中给出了这些建议背后的理由 专栏。有关如何回应建议的更多信息，请参阅the section called “响应建议”。

响应建议

建议是见解中最重要的部分。在分析的这一阶段，需要采取行动来解决性能问题。通常需要执行以下步骤：

1. 确定报告的性能问题是否表明存在实际问题。

   在某些情况下，问题可能是意料之中的且是良性的。例如，如果您使测试数据库承受极端的数据库负载， DevOpsGuru for RDS 会将负载报告为性能异常。但是，您无需纠正此异常，因为这是测试的预期结果。

   如果您确定问题需要回应，请转到下一步。

2. 确定是否实施该建议。

   在建议表中，有一列显示建议的操作。对于被动见解，这是被动异常详情页面上的我们的建议列。对于主动见解，这是主动见解页面上的推荐的自定义更改列。

   DevOpsGuru for RDS 提供了一系列建议，涵盖了几种潜在的问题场景。查看此列表后，确定哪项建议与当前情况更相关，并考虑将其进行应用。如果建议适合您的情况，请转到下一步。如果不适合，请跳过剩下的步骤，并通过手动方法解决问题。

3. 执行建议的操作。

   DevOpsRDS 版 Guru 建议您执行以下任一操作：

   - 执行特定的纠正操作。

     例如， DevOpsGuru for RDS 可能会建议您升级 CPU 容量、调整应用程序池设置或启用性能架构。

   - 调查问题的原因。

     通常， DevOpsGuru for RDS 建议您调查特定的 SQL 语句或等待事件。例如，建议可能是调查等待事件`io/table/sql/handler`。在《Amazon Aurora 用户指南》的使用 Aurora PostgreSQL 的等待事件进行调整或使用 Aurora MySQL 的等待事件进行调整中，或者在《Amazon RDS 用户指南》的使用 RDS for PostgreSQL 的等待事件进行调整中，查找列出的等待事件。然后执行建议的操作。

     > **Important**
     >
     > 我们建议您在修改生产实例之前在测试实例上测试所有更改。通过这种方式，您可以了解更改的影响。

使用 DevOps Guru 监控非关系数据库

DevOpsGuru 能够为您的非关系数据库或 NoSQL 数据库生成见解，帮助您根据最佳实践配置资源。例如， DevOpsGuru可以根据现有流量预测未来的需求，从而帮助您掌握容量规划。 DevOpsGuru 可以确定您使用的资源是否少于您的配置，并根据您的历史使用情况提供提高应用程序可用性的建议。这可以帮助您减少不必要的成本。

除了容量规划外， DevOpsGuru 还可以检测并帮助您解决操作问题，例如限制、交易冲突、条件检查失败以及 SDK 参数的改进领域。数据库通常与多个服务和资源相连， DevOpsGuru 可以使用基于标记或聚合的分组来关联您的应用程序结构以进行分析。 CloudFormation 异常可能涉及多个资源，这些资源都受同一个解决方案的影响。 DevOps Guru 能够关联不同的资源指标、配置、日志和事件。例如， DevOpsGuru 可以分析和关联来自 Lambda 函数的数据，该函数可能正在从表中 Amazon DynamoDB 读取或写入数据。通过这种方式， DevOpsGuru 可以监控多个相关资源，以检测异常情况，并为您的数据库解决方案提供有用的见解。

监控中的数据库操作 Amazon DynamoDB

下表显示了 DevOps Guru 监控的示例场景和见解。 Amazon DynamoDB

Amazon DynamoDB 用例	示例	指标
检测何时由于 AccountProvisionedWriteCapacityUtilization有大量的读取 AccountProvisionedReadCapacityUtilization 和写入请求而使用了很大比例的和。	Amazon DynamoDB 读取或写入请求的表消耗容量已达到表级限制。	AccountProvisionedReadCapacityUtilization, AccountProvisionedWriteCapacityUtilization
检测 Amazon DynamoDB 请求中的条件检查失败，原因是提供的条件表达式与数据库中的预期表达式不匹配。	条件检查失败是由表中的错误数据、严格的条件表达式或竞争条件造成的。	ConditionalCheckFailedRequests

监控中的数据库操作 Amazon ElastiCache

下表显示了 DevOps Guru 监控的示例场景和见解。 Amazon ElastiCache

DevOpsGuru 识别的场景	CloudWatch 监控的指标
检测 Amazon ElastiCache 集群何时由于对集群的需求变化而达到 Redis 或 Memcached 的计算限制。	CPUUtilization, 引擎CPUUtilization, 驱逐

与 CodeGuru Profiler 集成

本节概述了 Amazon DevOps Guru 如何与 Amazon P CodeGuru rofiler 集成。您可以在 DevOps Guru 控制台中将来自 CodeGuru Profiler 的推荐作为见解进行查看。

Amazon DevOps Guru 通过 EventBridge 托管规则与 Amazon CodeGuru Profiler 集成。 CodeGuru Profiler 将事件发送到。 EventBridge托管规则路由使用默认事件总线发送的事件。来自 CodeGuru Profiler 的每个入站事件都是一份主动异常报告。有关更多信息，请参阅使用 CodeGuru Pro EventBridge filer。

DevOpsGuru 通过以下方式支持入站活动。 EventBridge事件表明 DevOps Guru 发现的推荐发生了变化。 CodeGuru Profiler 每 24 小时发送一次心跳事件，以显示事件的连续性。事件携带 CodeGuru Profiler 推荐信息以及计算资源的元数据。有关事件生命周期的信息，请参阅 Amazon Event EventBridge s。

设置 DevOps Guru 时， DevOpsGuru 会在您的账户中创建 EventBridge 托管规则，用于路由来自其他服务的事件。这条规则是通往 DevOps大师的路线。当有入站事件时，将发送通知。

事件总线接收来自 DevOps Guru 等来源的事件，并将它们路由到与该事件总线关联的规则。有关事件总线的更多信息，请参阅事件总线。

有关某些参数的信息，请参阅 Amazon EventBridge 事件。

要在 DevOps Guru 中获取 P CodeGuru rofiler 见解，你必须具备以下条件。

- CodeGuru 必须启用 Profiler。有关启用 CodeGuru Profiler 的信息，请参阅设置 P CodeGuru rofil er。
- DevOps必须启用 Guru。有关启用 DevOps Guru 的信息，请参阅启用 DevOps G uru。
- 在 P CodeGuru rofiler 和 DevOps Guru 中，必须监控同一区域中的相同资源。

使用 AWS 资源定义应用程序

Amazon DevOps Guru 对覆盖范围内的资源进行分组，指定其分析哪些资源以获得运营见解。资源按 CloudFormation 堆栈中的资源或带标签的资源进行分组。你可以在设置 DevOps Guru 时选择堆栈或标签。您也可以稍后更新堆栈或标签。我们建议您将资源组视为应用程序。例如，您可能会将用于监控应用程序的所有资源定义在一个堆栈中。或者，您可以为数据库应用程序中使用的所有资源添加相同的标签。定义 DevOps Guru分析哪些资源的边界。集合中的所有资源都在这个边界内。您账户中不在资源集合中的任何资源都在边界之外，将不会接受分析。有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。

您可以通过三种方式定义包含应用程序资源的边界覆盖范围。

- 指定您的 AWS 账户和区域中所有支持的 AWS 资源。这使您的账户和区域成为您的资源边界。使用此选项， DevOpsGuru 可以分析您的账户和地区中所有支持的资源。一个堆栈中的所有资源都分组到一个应用程序中。任何不在堆栈中的资源都将分组到各自的应用程序中。
- 使用 CloudFormation 堆栈来指定应用程序中的资源。堆栈包含使用生成的资源 CloudFormation。在 DevOps Guru 中，你可以在账户中选择堆栈。您选择的每个堆栈中的资源将分组到一个应用程序中。 DevOpsGuru 会对堆栈中的所有资源进行分析，以获取见解。
- 使用 AWS 标签来指定应用程序中的资源。 AWS 标签包含一个键和一个值。在 DevOps Guru 中，选择一个标签键，然后选择一个或多个与该键配对的值。您可以使用这些值将资源分组到应用程序中。

有关更多信息，请参阅 在 DevOps Guru 中更新你的 AWS 分析覆盖范围。

主题

- 使用标签来识别 DevOps Guru 应用程序中的资源
- 使用 CloudFormation 堆栈来识别 DevOps Guru 应用程序中的资源

使用标签来识别 DevOps Guru 应用程序中的资源

您可以使用标签来识别 Amazon DevOps Guru 分析的 AWS 资源，并指定使用所选标签键和标签值对哪些资源进行分组以进行监控。在设置 DevOps Guru 或从 “已分析的资源” 页面中选择 “编辑分析的资源” 时，可以编辑这些配置。选择 “标签” 后，您可以选择希望 Amazon DevOps Guru 监控的特定标签密钥。要分析账户中的所有资源并使用标签值对资源进行分组，请选择所有账户资源。要使用标签值指定 DevOps Guru 要分析的资源，请选择选择特定的标签值。

> **Note**
>
> 选择所有账户资源且不存在标签值时，将单独对没有标签键的资源进行分组和分析。

可以使用标签的键来识别资源，然后使用带有该键的值将资源分组到您的应用程序中。例如，可以使用键devops-guru-applications来标记资源，然后为每个应用程序使用具有不同值的键。可以使用标签键值对devops-guru-applications/databasedevops-guru-applications/cicd和devops-guru-applications/monitoring来识别账户中的三个应用程序。每个应用程序都由包含相同标签键值对的相关资源组成。您可以使用资源所属的 AWS 服务为其添加标签。有关更多信息，请参阅 为 AWS 资源添加 AWS 标签。

在应用程序中为资源添加标签后，您可以按生成这些资源的标签来筛选您的见解。有关如何使用标签筛选见解的更多信息，请参阅查看 DevOps Guru 见解。

有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。

主题

- 什么是 AWS 标签？
- 使用标签定义 DevOps Guru 应用程序
- 在 DevOps Guru 中使用标签
- 为 AWS 资源添加 AWS 标签

什么是 AWS 标签？

标签可帮助您识别和整理 AWS 资源。许多 AWS 服务都支持标记，因此您可以为来自不同服务的资源分配相同的标签，以表明这些资源是相关的。例如，您可以为分配给函数的 Amazon DynamoDB 表资源分配相同的标签。 AWS Lambda 有关使用标签的更多信息，请参阅标记最佳实践白皮书。

每个 AWS 标签由两部分组成。

- 标签键 （例如，CostCenter、Environment、Project 或 Secret）。标签键区分大小写。
- 一个称为标签值的可选字段（例如，111122223333、Production 或团队名称）。省略标签值与使用空字符串相同。与标签键一样，标签值区分大小写。

这些被统称为键-值对。

使用标签定义 DevOps Guru 应用程序

要使用标签定义您的 Amazon DevOps Guru 应用程序，请将该标签添加到您账户中构成应用程序的 AWS 资源中。您的标签包含一个键和一个值。我们建议您为 DevOps Guru 分析的每个 AWS 资源添加一个具有相同密钥的标签。在标签中使用不同的值将资源分组到应用程序中。例如，您可以将带有密钥`devops-guru-analysis-boundary`的标签分配给覆盖范围内的所有 AWS 资源。使用带有该键的不同值来识别账户中的应用程序。您可以将值`containers`、`database`和`monitoring`用于三个应用程序。有关更多信息，请参阅 在 DevOps Guru 中更新你的 AWS 分析覆盖范围。

如果您使用 AWS 标签来指定要分析的资源，则可以使用只有一个密钥的标签。您可以将已配对的标签键与任何值配对。使用值将包含键的资源分组到您的操作应用程序中。

> **Important**
>
> 创建键时，键中字符的大小写可以是您选择的任意大小写。创建键后，它区分大小写。例如，DevOpsGuru 使用名为的密钥`devops-guru-rds`和名为的密钥`DevOps-Guru-RDS`，它们充当两个不同的密钥。您的应用程序中可能的键/值对可能为 `Devops-Guru-production-application/RDS` 或 `Devops-Guru-production-application/containers`。

在 DevOps Guru 中使用标签

指定用于 AWS 标识您希望 Amazon DevOps Guru 分析的 AWS 资源的标签，或指定用于标识将对哪些资源进行分组的标签值。这些资源是您的资源覆盖范围。您可以选择一个键和零个或多个值。

选择您的标签

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 打开导航窗格，然后展开设置。
3. 在已分析的资源中，选择编辑。
4. 如果您希望 DevOps Guru 分析包含您选择的标签的所有资源，请选择 “标签”。选择密钥，然后选择以下选项之一。

   - 所有账户资源-分析当前区域和账户中的所有 AWS 资源。具有所选标签键的资源按标签值（若有）进行分组。没有此标签键的资源将单独进行分组和分析。
   - 选择特定的标签值-将分析所有包含带有您选择的密钥的标签的资源。 DevOpsGuru 根据标签的值将您的资源分组到应用程序中。
5. 选择保存。

为 AWS 资源添加 AWS 标签

当您指定 AWS 标识您希望 DevOps Guru 分析的 AWS 资源的标签时，请选择与这些资源关联的标签。您可以使用每个资源所属的 AWS 服务或使用 AWS 标签编辑器为资源添加标签。

- 要使用资源服务管理标签，请使用资源所属服务的控制台或 SDK。 AWS Command Line Interface 例如，您可以为 Amazon Kinesis 直播资源或亚马逊 CloudFront 分发资源添加标签。以下是具有可添加标签的资源的服务的两个示例。DevOpsGuru 可以分析的大多数资源都支持标签。有关更多信息，请参阅 Amazon Kinesis 开发者指南中的为直播添加标签和亚马逊开发者指南中的为发行添加标签。 CloudFront 要了解如何为其他类型的资源添加标签，请参阅它们所属 AWS 服务的用户指南或开发者指南。

  > **Note**
  >
  > 在为 Amazon RDS 资源添加标签时，必须为数据库实例而不是集群添加标签。

- 您可以使用 AWS 标签编辑器按您所在地区的资源和特定 AWS 服务中的资源管理标签。有关更多信息，请参阅 AWS Resource Groups 和 Tags 用户指南中的标签编辑器。

为资源添加标签时，只能添加键，也可以添加键和值。例如，您可以`devops-guru-`为 DevOps 应用程序中的所有资源创建一个带有密钥的标签。也可以添加带有键`devops-guru-`和值RDS的标签，然后将该键值对添加到应用程序中的仅 Amazon RDS 资源。如果您想在控制台查看仅从应用程序中的 Amazon RDS 资源生成的见解，这会非常有用。

使用 CloudFormation 堆栈来识别 DevOps Guru 应用程序中的资源

您可以使用 AWS CloudFormation 堆栈来指定希望 DevOps Guru 分析哪些 AWS 资源。堆栈是作为一个单元管理的 AWS 资源集合。你选择的堆栈中的资源构成了你的 DevOps Guru 覆盖范围。对于您选择的每个堆栈，都会分析其受支持资源中的操作数据是否存在异常行为。然后将这些问题分组为相关异常以创建见解。每个见解都包含一项或多项建议，可帮助处理这些异常。您可以指定的最大堆栈数是 1000。有关更多信息，请参阅AWS CloudFormation 用户指南和在 DevOps Guru 中更新你的 AWS 分析覆盖范围中的使用堆栈。

选择堆栈后， DevOpsGuru 会立即开始分析您添加到堆栈中的任何资源。如果您从堆栈中移除一个资源，将不再对其进行分析。

如果您选择让 DevOps Guru 分析您账户中所有支持的资源（这意味着您的 AWS 账户和地区是您的 DevOps Guru 覆盖范围），Guru 会 DevOps分析您账户中所有支持的资源（包括堆栈中的资源）并创

建见解。根据不在堆栈中的资源的异常创建的见解在账户级别进行分组。如果见解是根据堆栈中资源的异常创建的，将在堆栈级别对其进行分组。有关更多信息，请参阅 了解异常行为如何分组为见解。

选择堆栈让 DevOps Guru 进行分析

通过选择创建资源的 CloudFormation 堆栈，指定您希望 Amazon DevOps Guru 分析的资源。您可以使用 AWS 管理控制台 或 SDK 执行此操作。

主题

- 选择堆栈让 DevOps Guru 进行分析（控制台）
- 选择堆栈让 Guru 进行分析（ DevOpsDevOpsGuru SDK）

选择堆栈让 DevOps Guru 进行分析（控制台）

您可以使用控制台添加 AWS CloudFormation 堆栈。

选择包含要分析的资源的堆栈

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 打开导航窗格，然后选择设置。
3. 在 DevOpsGuru 分析覆盖范围中，选择管理。
4. 如果您希望 DevOps Guru 分析您选择的CloudFormation 堆栈中的资源，请选择堆栈，然后选择以下选项之一。
   - 所有资源 — 分析您账户中堆栈中的所有资源。每个堆栈中的资源都分组到各自的应用程序中。系统不会分析账户中不在堆栈中的任何资源。
   - 选择堆栈 — 选择您希望 DevOps Guru 分析的堆栈。所选每个堆栈中的资源将分组到各自的应用程序中。您可以在查找堆栈中输入堆栈的名称以快速找到特定堆栈。您最多可以选择 1,000 个堆栈。
5. 选择保存。

选择堆栈让 Guru 进行分析（ DevOpsDevOpsGuru SDK）

要使用 Amazon DevOps Guru 软件开发工具包指定 CloudFormation 堆栈，请使用方法。`UpdateResourceCollection`有关更多信息，请参阅UpdateResourceCollection《Amazon DevOps Guru API 参考》。

与亚马逊合作 EventBridge

Amazon DevOps Guru 与亚马逊集成 EventBridge ，可通知您与见解和相应洞察更新相关的某些事件。来自 AWS 服务的事件几乎实时 EventBridge 地传送到。您可以编写简单规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。可自动触发的操作包括以下示例：

- 调用函数 AWS Lambda
- 调用 Amazon Elastic Compute Cloud 运行命令
- 将事件中继到 Amazon Kinesis Data Streams
- 激活 Step Functions 状态机
- 通知 Amazon SNS 或 Amazon SQS

您可以选择以下任一预定义模式来筛选事件，或者创建自定义模式规则以在支持的 AWS 资源中启动操作。

- DevOps Guru 新洞察开启
- DevOps Guru 新异常协会
- DevOps Guru Insight 严重性已
- DevOps Guru 新推荐已创建
- DevOps 大师洞察已关闭

DevOpsGuru 活动

以下是来自 DevOps Guru 的示例事件。尽最大努力发布事件。要了解有关事件模式的更多信息，请参阅 Amazon EventBridge 或 Amaz on EventBridge 事件模式入门。

DevOps Guru New Insight 公开活动

当 DevOps Guru 打开新的见解时，它会发送以下事件。

```
{
    "version" : "0",
    "id" : "08108845-ef90-00b8-1ad6-2ee5570ac6c4",
    "detail-type" : "DevOps Guru New Insight Open",
    "source" : "aws.devops-guru",
    "account" : "123456789012",
```

```
    "time" : "2021-11-01T17:06:10Z",
    "region" : "us-east-1",
    "resources" : [ ],
    "detail" : {
      "insightSeverity" : "high",
      "insightDescription" : "ApiGateway 5XXError Anomalous In Stack TestStack",
      "insightType" : "REACTIVE",
      "anomalies" : [
        {
          "startTime" : "1635786000000",
          "id" : "AL41JDFFQPYlZlXD8cpREkAAAAF83HGGgC9TmTr9lbfJ7sCiISlWMeFCbHY_XXXX",
          "sourceDetails" : [
            {
              "dataSource" : "CW_METRICS",
              "dataIdentifiers" : {
                "period" : "60",
                "stat" : "Average",
                "unit" : "None",
                "name" : "5XXError",
                "namespace" : "AWS/ApiGateway",
                "dimensions" : [
                  {
                    "name" : "ApiName",
                    "value" : "Test API Service"
                  },
                  {
                    "name" : "Stage",
                    "value" : "prod"
                  }
                ]
              }
            }
          ]
        }
      ],
      "accountId" : "123456789012",
      "messageType" : "NEW_INSIGHT",
      "insightUrl" : "https://us-east-1.console.aws.amazon.com/devops-guru/#/insight/
reactive/AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "startTime" : "1635786120000",
      "insightId" : "AIYH6JxdbgkcG0xJmypiL4MAAAAAAAAAL0SLEjkxiNProXWcsTJbLU07EZ7XXXX",
      "region" : "us-east-1"
    }
```

```
  },
```

针对高严重性的新见解自定义示例事件模式

规则使用事件模式来选择事件并将事件路由到目标。以下是 DevOps Guru 事件模式示例。

```
{
  "source": [
    "aws.devops-guru"
  ],
  "detail-type": [
    "DevOps Guru New Insight Open"
  ],
  "detail": {
    "insightSeverity": [
         "high"
         ]
  }
}
```

更新 DevOps Guru 设置

您可以更新以下 Amazon DevOps Guru 设置：

- 你的 DevOps Guru 报道。这决定了将分析账户中的哪些资源。
- 通知。这决定了使用哪些 Amazon 简单通知服务主题来通知您重要的 DevOps Guru 事件。
- 增强见解的特征。这包括日志异常检测、加密和您的 AWS Systems Manager 集成设置。这决定了 DevOps Guru 是否显示日志数据、您是否使用其他安全密钥以及是否在 Systems Manager 中 OpsCenter 为每个新见解创建一个 OpsItem 。

主题

- 更新您的管理账户设置
- 在 DevOps Guru 中更新你的 AWS 分析覆盖范围
- 在 DevOps Guru 中更新你的通知
- 筛选你的 DevOps Guru 通知
- 在 DevOps Gur AWS Systems Manager u 中更新集成
- 在 Guru 中 DevOps更新日志异常检测
- 在 DevOps Guru 中更新加密设置

更新您的管理账户设置

您可以为组织中的帐户配置 DevOps Guru。如果您尚未注册委派管理员，则可以通过选择注册委派管理员进行注册。有关注册委派管理员的更多信息，请参阅启用 DevOps Guru。

在 DevOps Guru 中更新你的 AWS 分析覆盖范围

您可以更新 DevOps Guru 分析您账户中的哪些 AWS 资源。为此，请在控制台中导航到已分析资源页面，然后选择编辑。有关更多信息，请参阅 查看已分析的资源。

在 DevOps Guru 中更新你的通知

设置亚马逊简单通知服务主题，用于通知您有关重要的 Amazon DevOps Guru 事件。您可以从账户中已存在的主题名称列表中进行选择，输入 DevOps Guru 在您的 AWS 账户中创建的新主题的名称，或

者输入您所在地区 AWS 任何账户中现有主题的 Amazon 资源名称 (ARN)。如果您为不在您的账户中的主题指定了 ARN，则必须通过向其添加 IAM 策略来授予 DevOps Guru 访问该主题的权限。有关更多信息，请参阅 Amazon SNS 主题的权限。最多可以指定两个主题。

DevOpsGuru 会发送有关以下更新的通知：

- 创建了新的见解。
- 一个新的异常被添加到见解中。
- 见解的严重性从 Low 或升级 Medium 到 High。
- 见解的状态从“持续”变为“已解决”。
- 识别了对见解的建议。

DevOps当您尝试向 Guru 账户添加资源时，如果选定的 CloudFormation 堆栈或标签密钥无效，DevOpsGuru 还会发送通知。

您可以选择接收有关各种问题更新的 Amazon SNS 通知，也可以选择仅在问题打开、关闭或严重性发生变化时接收 Amazon SNS 通知。默认情况下，您会接收关于所有更新的通知。

要更新通知，请先导航到通知页面，然后选择是添加、删除还是更新针对 Amazon SNS 通知主题的配置。

主题

- 在 DevOps Guru 控制台中导航到通知设置
- 在 Guru 控制台中添加 Amazon SNS 通知主题 DevOps
- 在 Guru 控制台中移除 Amazon SNS 通知主题 DevOps
- 更新 Amazon SNS 通知配置
- 添加到 Amazon SNS 主题的权限

在 DevOps Guru 控制台中导航到通知设置

要更新通知，必须先导航到通知设置部分。

导航到通知设置部分

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 在导航窗格中，选择设置。

“设置”页面包括通知部分，其中包含有关已配置 Amazon SNS 主题的信息。

在 Guru 控制台中添加 Amazon SNS 通知主题 DevOps

在 Guru 控制台中添加 Amazon SNS 通知主题 DevOps

1. the section called “在 DevOps Guru 控制台中导航到通知设置”.
2. 选择 Add notification（添加通知）。
3. 要添加 Amazon SNS 主题，请执行以下任一操作。
   - 选择使用电子邮件生成新的 SNS 主题。然后，在指定电子邮箱地址中，输入要接收通知的电子邮箱地址。要输入其他电子邮箱地址，请选择添加新的电子邮箱。
   - 选择使用现有 SNS 主题。然后，从 “选择 AWS 账户中的主题” 中，选择要使用的主题。
   - 选择使用现有 SNS 主题 ARN 来指定来自另一账户的现有主题。然后，在输入主题的 ARN 中，输入主题 ARN。ARN 是主题的 Amazon 资源名称。您可以在不同的账户中指定主题。如果使用另一个账户中的主题，则必须向该主题添加资源策略。有关更多信息，请参阅 Amazon SNS 主题的权限。
4. 选择 Save。

在 Guru 控制台中移除 Amazon SNS 通知主题 DevOps

在 Guru 控制台中移除 Amazon SNS 主题 DevOps

1. the section called “在 DevOps Guru 控制台中导航到通知设置”.
2. 选择选择现有主题。
3. 从下拉菜单中，选择要移除的主题。
4. 选择移除。
5. 选择保存。

更新 Amazon SNS 通知配置

Guru 中的 DevOps Amazon SNS 通知主题有两种类型的通知配置。可以选择接收所有严重性级别的通知，也可以选择仅接收严重性级别为高和中的通知。还可以选择接收各种有关更新的通知，或仅接收某些类型的更新通知。

当您选择接收有关各种问题更新的Amazon SNS通知时， DevOpsGuru 会发送有关以下更新的通知：

- 创建了新的见解。
- 一个新的异常被添加到见解中。
- 见解的严重性从 Low 或升级 Medium 到 High。
- 见解的状态从“持续”变为“已解决”。
- 识别了对见解的建议。

默认情况下，您只会收到严重级别为高和中的通知，并且会收到有关各种更新的通知。

更新 Amazon SNS 通知主题的通知配置

1. the section called “在 DevOps Guru 控制台中导航到通知设置”.
2. 选择选择现有主题。
3. 从下拉菜单中，选择要对其进行更新的主题。
4. 选择所有严重性级别以接收严重性级别为“高”、“中”和“低”的通知，也可以选择仅高和中以接收严重性级别为“高”和“中”的通知。
5. 选择见解有任何更新时通知我，也可以选择在见解打开或关闭时或者严重性级别从“低”或“中”变为“高”时通知我。
6. 选择保存。

添加到 Amazon SNS 主题的权限

Amazon SNS 主题是一种包含 AWS Identity and Access Management (IAM) 资源策略的资源。当您在此处指定主题时， DevOpsGuru 会将以下权限附加到其资源策略中。

```
{
    "Sid": "DevOpsGuru-added-SNS-topic-permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "region-id.devops-guru.amazonaws.com"
    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:region-id:topic-owner-account-id:my-topic-name",
    "Condition" : {
      "StringEquals" : {
```

```
        "AWS:SourceArn": "arn:aws:devops-guru:region-id:topic-owner-account-
id:channel/devops-guru-channel-id",
        "AWS:SourceAccount": "topic-owner-account-id"
    }
  }
}
```

DevOpsGuru 需要这些权限才能使用主题发布通知。如果您不想拥有该主题的这些权限，则可以放心地将其删除，主题将继续按照您选择之前的方式运行。但是，如果删除了这些附加权限，DevOpsGuru 将无法使用该主题生成通知。

筛选你的 DevOps Guru 通知

您可以通过the section called “更新 Amazon SNS 通知配置”或使用 Amazon SNS 订阅筛选策略来筛选您的 DevOps Guru 通知。

主题

- 使用 Amazon SNS 订阅筛选策略来筛选通知
- Amazon Guru 筛选过的 Amazon SNS 通知示例 DevOps

使用 Amazon SNS 订阅筛选策略来筛选通知

您可以创建亚马逊简单通知服务 (Amazon SNS) Simple Notification 订阅筛选政策，以减少从亚马逊 Guru 收到的通知数量。 DevOps

使用筛选策略来指定您接收的通知类型。您可以使用以下关键字来筛选 Amazon SNS 消息。

- NEW_INSIGHT — 在创建新见解时接收通知。
- CLOSED_INSIGHT — 在现有见解关闭时接收通知。
- NEW_RECOMMENDATION — 在根据见解创建新建议时接收通知。
- NEW_ASSOCIATION — 在从见解中检测到新异常时接收通知。
- CLOSED_ASSOCIATION — 在现有异常关闭时接收通知。
- SEVERITY_UPGRADED — 在见解的严重性升级时接收通知

有关如何创建亚马逊 SNS 订阅筛选策略的信息，请参阅 Amazon Simple Notification Service 开发人员指南中的亚马逊 SNS 订阅筛选策略。在筛选策略中，您可以指定一个带有该策略 MessageType 的关

键字。例如，以下内容将出现在筛选条件中，该筛选条件指定 Amazon SNS 主题仅在从见解中检测到新异常时才发送通知。

```
{
  "MessageType":["NEW_ ASSOCIATION"]
}
```

Amazon Guru 筛选过的 Amazon SNS 通知示例 DevOps

以下是一个来自具有筛选策略的 Amazon SNS 主题的 Amazon Simple Notification Service (Amazon SNS) 通知的示例。它的 `MessageType` 被设置为 `NEW_ASSOCIATION`，因此只有在从见解中检测到新的异常时，它才会发送通知。

```
{
      "accountId": "123456789012",
      "region": "us-east-1",
      "messageType": "NEW_ASSOCIATION",
      "insightId": "ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-Function duration due to increased number of invocations",
      "insightUrl": "https://us-east-1.console.aws.amazon.com/devops-guru/insight/
reactive/ADyf4FvaVNDzu9MA2-IgFDkAAAAAAAAAEGpJd5sjicgauU2wmAlnWUyyI2hiO5it",
      "insightType": "REACTIVE",
      "insightDescription": "At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-Function had\n an increased duration anomaly possibly caused by
 the Lambda function invocation increase. DevOps Guru has detected this is a repeated
 insight. DevOps Guru treats repeated insights as 'Low Severity'.",
      "startTime": 1628767500000,
      "startTimeISO": "2023-03-29T22:00:00Z",
      "anomalies": [
        {
          "id": "AG2n8ljW74BoI1CHu-m_oAgAAAF7Ohu24N4Yro69ZSdUtn_alzPH7VTpaL30JXiF",
          "startTime": 1628767500000,
          "startTimeISO": "2023-03-29T22:00:00Z",
          "openTime": 1680127740000,
          "openTimeISO": "2023-03-29T22:09:00Z",
          "sourceDetails": [
            {
              "dataSource": "CW_METRICS",
              "dataIdentifiers": {
                "namespace": "AWS/SQS",
                "name": "ApproximateAgeOfOldestMessage",
```

```
                "stat": "Maximum",
                "unit": "None",
                "period": "60",
                "dimensions": "{\"QueueName\":\"FindingNotificationsDLQ\"}"
              }
            }
          ],
          "associatedResourceArns":[
           "arn:aws:sns:us-east-1:123456789012:DevOpsGuru-insights-sns"
          ]
        }
      ],
      "resourceCollection":{
      "cloudFormation":{
         "stackNames":[
            "CapstoneNotificationPublisherEcsApplicationInfrastructure"
          ]
        }
      }
}
```

在 DevOps Gur AWS Systems Manager u 中更新集成

您可以在中 OpsItem 为每个新见解启用创建 AWS Systems Manager OpsCenter。 OpsCenter 是一个集中式系统，您可以在其中查看、调查和审查操作工作项目 (OpsItems)。f OpsItems or your insights 可以帮助您管理工作，以解决触发创建每项见解的异常行为。有关更多信息，请参阅《AWS Systems Manager 用户指南》 OpsItem中的AWS Systems Manager OpsCenter和使用。

> **Note**
>
> 如果您更改的标签字段的键或值 OpsItem， DevOpsGuru 将无法对其进行 OpsItem更新。例如，如果您将 from 的标签更改为 OpsItem 其他标签，那么 DevOps Guru 就无法对其进行更新。`"aws:RequestTag/DevOps-GuruInsightSsmOpsItemRelated": "true"` OpsItem

管理 Systems Manager 集成

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 在导航窗格中，选择设置。

3. 在AWS Systems Manager 集成中，选择 “启用 DevOps Guru”， OpsCenter 为每个见解创建一个 AWS OpstItem inin，为每个新见解 OpsItem 创建一个。取消选择该选项可停止为每个新见解OpsItem创建一个。

您需要为在自己的账户中 OpsItems 创建账号付费。有关更多信息，请参阅AWS Systems Manager 定价。

在 Guru 中 DevOps更新日志异常检测

管理日志异常检测设置

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 在导航窗格中，选择设置。
3. 在 “日志异常检测” 中，选择 “通过授予 DevOps Guru 显示与洞察关联的日志数据的权限来启用日志异常检测”。 让 DevOps Guru 显示与见解相关的日志数据。

在 DevOps Guru 中更新加密设置

您可以更新加密设置以使用 AWS 自有密钥或 AWS KMS 客户管理的密钥。从现有客户托管 AWS KMS 密钥切换到新的客户托管 AWS KMS 密钥时， DevOpsGuru 会自动开始使用新密钥加密新摄取的元数据。历史数据将使用先前配置的客户托管 AWS KMS 密钥保持加密状态。

> **Note**
>
> 如果您撤销授权，或者禁用或删除之前的 AWS KMS 密钥， DevOpsGuru 将无法访问由此密钥加密的任何数据，并且您可能会在执行读取操作`AccessDeniedException`时看到。

管理加密设置

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 在导航窗格中，选择设置。
3. 在加密部分，选择编辑加密。
4. 选择要用于保护数据的加密类型。您可以使用默认 AWS 拥有的密钥、选择现有的客户托管密钥或创建新的客户托管 AWS KMS 密钥。

5. 选择保存。

加密是 DevOps Guru 安全的重要组成部分。有关更多信息，请参阅 the section called “数据保护”。

查看通知

DevOpsGuru 中有不同类型的通知。

主题

- 新见解
- 已关闭见解
- 新关联
- 新建议
- 严重性升级
- 资源验证失败

本页各节显示了每种通知类型的示例。

新见解

有关新见解的通知包含以下信息：


```
{
   "accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-4",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"DevOps Guru has detected this is a repeated insight. DevOps
 Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680148920000,
   "startTimeISO": "2023-03-30T04:02:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime": 1680148800000,
         "startTimeISO": "2023-03-30T04:00:00Z",
```

```
         "openTime": 1680148920000,
         "openTimeISO": "2023-03-30T04:02:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
                  "name":"ApproximateAgeOfOldestMessage",
                  "namespace":"AWS/SQS",
                  "period":"60",
                  "stat":"Maximum",
                  "unit":"None",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        },
   }
}
```

已关闭见解

已关闭见解的通知包含以下信息：

```
{
"accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"CLOSED_INSIGHT",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "DynamoDB table writes are under utilized in mock-stack",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription":"DynamoDB table writes are under utilized",
```

```
    "insightSeverity":"medium",
    "startTime": 1670612400000,
    "startTimeISO": "2022-12-09T19:00:00Z",
    "endTime": 1679994000000,
    "endTimeISO": "2023-03-28T09:00:00Z",
    "anomalies":[
       {
          "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
          "startTime": 1665428400000,
          "startTimeISO": "2022-10-10T19:00:00Z",
          "endTime": 1679986800000,
          "endTimeISO": "2023-03-28T07:00:00Z",
          "openTime": 1670612400000,
          "openTimeISO": "2022-12-09T19:00:00Z",
          "closeTime": 1679994000000,
          "closeTimeISO": "2023-03-28T09:00:00Z",
          "description":"Empty receives while messages are available",
          "anomalyResources":[
             {
                "type":"AWS::SQS::Queue",
                "name":"SampleQueue"
             }
          ],
          "sourceDetails":[
             {
                "dataSource":"CW_METRICS",
                "dataIdentifiers":{
                "name":"NumberOfEmptyReceives",
                   "namespace":"AWS/SQS",
                   "period":"60",
                   "stat":"Sum",
                   "unit":"COUNT",
                   "dimensions":"{\"QueueName\":\"SampleQueue\"}"
                }
             }
          ],
         "associatedResourceArn": [
             "arn:aws:sqs:us-east-1:123456789101:SampleQueue"
         ]
       }
    ],
    "resourceCollection":{
         "cloudFormation":{
             "stackNames":[
```

```
                "SampleApplication"
            ]
        }
    }
}
```

新关联

新关联的通知包含以下信息：

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"NEW_ASSOCIATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightName": "Repeated Insight: Anomalous increase in Lambda
 ApigwLambdaDdbStack-22-GetOneFunction duration due to increased number of
 invocations",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
   "insightType":"REACTIVE",
   "insightDescription":"At March 29, 2023 22:02 GMT, Lambda function
 ApigwLambdaDdbStack-22-GetOneFunction had\nan increased duration anomaly possibly
 caused by the Lambda function invocation increase. DevOps Guru has detected this is a
 repeated insight. DevOps Guru treats repeated insights as 'Low Severity'.",
   "insightSeverity":"medium",
   "startTime": 1680127200000,
   "startTimeISO": "2023-03-29T22:00:00Z",
   "anomalies":[
      {
         "id":"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
         "startTime":1672945500000,
         "startTimeISO": "2023-03-29T22:00:00Z",
         "openTime": 1680127740000,
         "openTimeISO": "2023-03-29T22:09:00Z",
         "sourceDetails":[
            {
               "dataSource":"CW_METRICS",
               "dataIdentifiers":{
               "namespace":"AWS/SQS",
                  "name":"ApproximateAgeOfOldestMessage",
                  "stat":"Maximum",
                  "unit":"None",
```

```
                  "period":"60",
                  "dimensions":"{\"QueueName\":\"SampleQueue\"}"
               }
            }
         ],
         "associatedResourceArns":[
            "arn:aws:sqs:eu-west-1:123456789101:SampleQueue"
         ]
      }
   ],
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

新建议

新建议的通知包含以下信息：

```
{
   "accountId":"123456789101",
   "region":"us-east-1",
   "messageType":"NEW_RECOMMENDATION",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightName": "Recreation of AWS SDK Service Clients",
   "insightUrl":"https://us-east-1.console.aws.amazon.com/devops-guru/insight/
proactive/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
   "insightType":"PROACTIVE",
   "insightDescription": "Usually for a given service you can create one [AWS SDK
 service client](https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/creating-
clients.html) and reuse that client across your entire service.\n\nWhen instead you
 create a new AWS SDK service client for each call (e.g. for DynamoDB) it\u0027s
 generally a waste of CPU time.",
   "insightSeverity":"medium",
   "startTime": 1680125893576,
   "startTimeISO": "2023-03-29T21:38:13.576Z",
   "recommendations":[
      {
         "name":"Tune Availability Zones of your Lambda Function",
```

```
        "description":"Based on your configurations, we recommend that you set
 SampleFunction to be deployed in at least 3 Availability Zones to maintain Multi
 Availability Zone Redundancy.",
        "reason":"Lambda Function SampleFunction is currently only deployed to 2
 unique Availability zones in a region with 7 total Availability zones.",
        "link":"https://docs.aws.amazon.com/lambda/latest/dg/configuration-vpc.html",
        "relatedAnomalies":[
           {
              "sourceDetails":{
                   "cloudWatchMetrics":null
              },
              "resources":[
                 {
                    "name":"SampleFunction",
                    "type":"AWS::Lambda::Function"
                 }
              ],
              "associatedResourceArns": [
                 "arn:aws:lambda:arn:123456789101:SampleFunction"
              ]
           }
        ]
     }
  ],
  "resourceCollection": {
       "cloudFormation": {
       "stackNames":[
           "SampleApplication"
        ]
     }
  }
}
```

严重性升级

严重性升级的通知包含以下信息：

```
{
"accountId":"123456789101",
   "region":"eu-west-1",
   "messageType":"SEVERITY_UPGRADED",
   "insightId":"a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
```

```
   "insightName": "Repeated Insight: ApiGateway 5XXError Anomalous In Application
 CanaryCommonResources-123456789101-LogAnomaly-11",
   "insightUrl":"https://eu-west-1.console.aws.amazon.com/devops-guru/insight/reactive/
a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
   "insightType":"REACTIVE",
   "insightDescription": "DevOps Guru has detected this is a repeated insight. DevOps
 Guru will treat future occurrences of this insight as 'Low Severity' for the next 7
 days.",
   "insightSeverity":"high",
   "startTime": 1680127320000,
   "startTimeISO": "2023-03-29T22:02:00Z",
   "resourceCollection":{
        "cloudFormation":{
            "stackNames":[
                "SampleApplication"
            ]
        }
   }
}
```

资源验证失败

您可以使用 CloudFormation 堆栈和 AWS 标签来筛选和识别您希望 DevOps Guru 分析的 AWS 资源。当您选择无效的堆栈或标签让 DevOps Guru 用来标识资源时，DevOpsGuru 会创建SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE通知。当您指定的标签或堆栈名称没有与之关联的资源时，就会发生这种情况。要充分利用 DevOps Guru 筛选方法，请选择与之关联的资源的堆栈和标签。

```
{
    "accountId":"123456789101",
    "region":"eu-west-1",
    "messageType":"SELECTED_RESOURCE_FILTER_VALIDATION_FAILURE",
    "ResourceFilterType": "Tags",
    "InvalidResourceNames": [
         "Devops-Guru-tag-key-tag-value"
    ],
    "awsInsightSource": "aws.devopsguru"
}
```

查看 DevOps Guru 分析的资源

DevOpsGuru 使用该`ListMonitoredResources`操作提供了正在分析的资源名称及其应用程序边界的列表。这些信息是使用 DevOps Guru AWS 服务关联角色从 Amazon CloudWatch 和其他服务收集的。 AWS CloudTrail

请注意，即使用户没有访问其他服务（例如 AWS Lambda 或 Amazon RDS）的明确权限，只要允许该`ListMonitoredResources`操作， DevOpsGuru 仍会提供该服务的资源列表。 APIs

主题

- 在 DevOps Guru 中更新你的 AWS 分析覆盖范围
- 为用户移除已分析资源的视图

在 DevOps Guru 中更新你的 AWS 分析覆盖范围

您可以更新 DevOps Guru 分析您账户中的哪些 AWS 资源。所分析的资源构成了你的 DevOps Guru 覆盖范围。当您指定边界时，您的资源将在应用程序中进行分组。您有四个边界涵盖范围选项。

- 选择让 DevOps Guru 分析您账户中所有支持的资源。您账户中堆栈中的所有资源都将分组到一个应用程序中。如果账户中有多个堆栈，则每个堆栈中的资源将构成自己的应用程序。如果账户中的任何资源不在堆栈中，则会将它们分组到自己的应用程序中。
- 通过选择定义这些资源的 AWS CloudFormation 堆栈来指定资源。如果你这样做， DevOpsGuru 会分析你选择的堆栈中指定的所有资源。如果账户中的资源不是由所选堆栈定义的，则不会对其进行分析。有关更多信息，请参阅CloudFormation 用户指南和确定 DevOps Guru 的覆盖范围中的使用堆栈。
- 使用 AWS 标签指定资源。 DevOpsGuru 要么分析您的账户和区域中的所有资源，要么分析包含您选择的标签密钥的所有资源。资源根据选定的标签值进行分组。有关更多信息，请参阅 使用标签来识别 DevOps Guru 应用程序中的资源。
- 指定不分析任何资源，这样您就可以不再因资源分析而产生费用。

> **Note**
>
> 如果您更新报道以停止分析资源，则如果您查看 DevOps Guru过去生成的现有见解，则可能会继续产生少量费用。这些费用与用于检索和显示见解信息的 API 调用有关。有关更多信息，请参阅 Amazon DevOps Guru 定价。

DevOpsGuru 支持与支持的服务关联的所有资源。有关支持的服务和资源的更多信息，请参阅 Amazon DevOps Guru 定价。

管理您的 DevOps Guru 分析覆盖范围

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 展开导航窗格中的已分析资源。
3. 选择编辑。
4. 请选择以下任一涵盖范围选项。

   - 如果您希望 DevOps Guru 分析您的账户和地区中所有支持的资源，请选择所有 AWS 账户资源。如果您选择此选项，则您的 AWS 账户就是您的资源分析覆盖范围。账户中每个堆栈中的所有资源都分组到各自的应用程序中。任何不在堆栈中的剩余资源都将分组到各自的应用程序中。
   - 如果您希望 DevOps Guru 分析您选择的CloudFormation 堆栈中的资源，请选择堆栈，然后选择以下选项之一。
     - 所有资源 — 分析您账户中堆栈中的所有资源。每个堆栈中的资源都分组到各自的应用程序中。系统不会分析账户中不在堆栈中的任何资源。
     - 选择堆栈 — 选择您希望 DevOps Guru 分析的堆栈。所选每个堆栈中的资源将分组到各自的应用程序中。您可以在查找堆栈中输入堆栈的名称以快速找到特定堆栈。您最多可以选择 1,000 个堆栈。

     有关更多信息，请参阅 使用 CloudFormation 堆栈来识别 DevOps Guru 应用程序中的资源。
   - 如果您希望 DevOps Guru 分析包含您选择的标签的所有资源，请选择 “标签”。选择密钥，然后选择以下选项之一。
     - 所有账户资源 — 分析当前区域和账户中的所有 AWS 资源。具有所选标签键的资源按标签值（若有）进行分组。没有此标签键的资源将单独进行分组和分析。
     - 选择特定的标签值-将分析所有包含带有您选择的密钥的标签的资源。 DevOpsGuru 根据标签的值将您的资源分组到应用程序中。

     有关更多信息，请参阅 使用标签来识别 DevOps Guru 应用程序中的资源。
   - 如果您不希望 DevOps Guru 分析任何资源，请选择 “无”。此选项禁用 DevOps Guru，这样您就可以停止因资源分析而产生费用。
5. 选择保存。

为用户移除已分析资源的视图

即使用户没有访问其他服务（例如 Lambda 或 Amazon RDS）的明确权限，只要允许该`ListMonitoredResources`操作， DevOpsGuru 仍会提供该服务的资源列表。 APIs 要更改此行为，您可以更新您 AWS 的 IAM 策略以拒绝此操作。

```
{
            "Sid": "DenyListMonitoredResources",
            "Effect": "Deny",
            "Action": [
                "devops-guru:ListMonitoredResources"
            ]
}
```

DevOpsGuru 最佳实践

以下最佳实践可以帮助您理解、诊断和修复 Ama DevOps zon Guru 检测到的异常行为。使用最佳实践在 DevOps Guru 控制台中了解见解来解决 DevOps Guru 检测到的操作问题。

- 在见解的时间轴视图中，首先查看突出显示的指标。它们通常是问题的关键指标。
- 使用 Amazon CloudWatch 查看在洞察中第一个突出显示的指标之前出现的指标，以查明行为何时以及如何发生变化。这可以帮助您诊断和解决问题。
- 要获取 Amazon RDS 资源，请查看“性能详情”指标。通过将计数器指标与数据库负载相关联，可以获得有关性能问题的详细信息。有关更多信息，请参阅使用 G DevOpsurufor Amazon RDS 分析性能异常。
- 同一指标的多个维度通常可能是异常的。查看图形视图中的维度，以更深入地了解问题。
- 在见解的事件部分查看创建见解时发生的部署或基础架构事件。了解在见解出现异常行为时发生了哪些事件可以帮助您了解和诊断问题。
- 在操作系统中寻找与线索见解差不多同时出现的工单。
- 在见解中，阅读建议并访问建议中的链接。这些通常包含故障排除步骤，可以帮助您快速诊断和解决问题。
- 除非已经解决了问题，否则不要忽略已解决的见解。每天一次，查看新的见解，即使这些见解已经得到解决。尝试尽可能多地了解这些见解背后的根本原因。寻找一种可能是系统性问题征兆的模式。如果系统性问题得不到解决，它将来可能会造成更严重的问题。立即修复暂时性问题可以帮助防止将来发生更严重的事件。

Amazon DevOps Guru 中的安全

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon DevOps Guru 的合规计划，请参阅按合规计划划分的 AWS 范围内的服务 AWS 按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 DevOps Guru 时如何应用分担责任模型。以下主题向您展示如何配置 DevOps Guru 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 DevOps Guru 资源。

主题

- Amazon DevOps Guru 中的数据保护
- Amazon DevOps Guru 的身份和访问管理
- 记录和监控 DevOps Guru
- DevOpsGuru 和接口 VPC 终端节点 ()AWS PrivateLink
- DevOpsGuru 的基础设施安全
- Amazon DevOps Guru 的韧性

Amazon DevOps Guru 中的数据保护

AWS 分担责任模式分适用于 Amazon DevOps Guru 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您 AWS 服务 使用控制台、API 或与 DevOps Guru 或其他人合作时。 AWS CLI AWS SDKs在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

DevOpsGuru 中的数据加密

加密是 DevOps Guru 安全的重要组成部分。某些加密（例如，针对传输中的数据的加密）是默认提供的，无需您执行任何操作。其他加密（例如，针对静态数据的加密）可在创建项目或构建时进行配置。

- 传输中的数据加密：客户与 Guru 之间以及 DevOps Guru 与其下游依赖关系之间 DevOps的所有通信均使用 TLS 进行保护，并使用签名版本 4 签名流程进行身份验证。所有 DevOps Guru 端点都使用由管理的 AWS 私有证书颁发机构证书。有关更多信息，请参阅签名版本 4 签名流程和什么是 ACM PCA。
- 静态数据加密：对于 DevOps Guru 分析的所有 AWS 资源，亚马逊 CloudWatch 指标和数据、资源 IDs和 AWS CloudTrail 事件均使用亚马逊 S3、亚马逊 DynamoDB 和 Amazon Kinesis 存储。如果使用 CloudFormation 堆栈来定义所分析的资源，则还会收集堆栈数据。 DevOpsGuru 使用亚马逊 S3、DynamoDB 和 Kinesis 的数据保留策略。存储在 Kinesis 中的数据最多可以保留一年，具体取决于所设置的策略。存储在 Amazon S3 和 DB 中的数据将存储一年。

  存储的数据使用亚马逊 S3、DynamoDB 和 Kinesis 的 data-at-rest加密功能进行加密。

客户托管密钥： DevOpsGuru 支持加密客户内容和敏感元数据，例如使用客户托管密钥从日志中生成的 CloudWatch 日志异常。此功能为您提供了添加自我管理安全层的选项，以帮助您满足组织的合规性和监管要求。有关在 DevOps Guru 设置中启用客户托管密钥的信息，请参阅the section called “更新加密”。

由于您可以完全控制这层加密，因此可以执行以下任务：

- 制定和维护关键策略
- 建立和维护 IAM 策略和授权
- 启用和禁用密钥策略
- 轮换加密材料
- 添加 标签
- 创建密钥别名
- 安排密钥删除

有关更多信息，请参阅《 AWS Key Management Service 开发人员指南》中的客户托管密钥。

> **Note**
>
> DevOpsGuru 使用 AWS 自有密钥自动启用静态加密，从而免费保护敏感元数据。但是，使用客户管理的密钥需要 AWS KMS 付费。有关定价的更多信息，请参阅定 AWS Key Management Service 价。

DevOpsGuru 如何使用补助金 AWS KMS

DevOpsGuru 需要获得授权才能使用您的客户托管密钥。

当您选择使用客户托管密钥启用加密时， DevOpsGuru 会通过向发送 CreateGrant 请求来 AWS KMS 代表您创建授权。中的授权 AWS KMS 用于让 DevOps Guru 访问客户账户中的 AWS KMS 密钥。

DevOpsGuru 需要获得授权才能使用您的客户托管密钥进行以下内部操作：

- 向发送 DescribeKey 请求， AWS KMS 以验证在创建跟踪器或地理围栏集合时输入的对称客户托管 KMS 密钥 ID 是否有效。
- 向发送 GenerateDataKey 请求 AWS KMS 以生成由您的客户托管密钥加密的数据密钥。
- 将 Decrypt 请求发送 AWS KMS 到以解密加密的数据密钥，以便它们可用于加密您的数据。

您可以随时撤销授予访问权限，或删除服务对客户托管密钥的访问权限。如果您这样做，DevOpsGuru 将无法访问由客户托管密钥加密的任何数据，这会影响依赖该数据的操作。例如，如果您尝试获取 DevOps Guru 无法访问的加密日志异常信息，则该操作将返回错误 AccessDeniedException 。

在 DevOps Guru 中监控您的加密密钥

当您将 AWS KMS 客户托管密钥与 DevOps Guru 资源一起使用时，您可以使用 AWS CloudTrail 或 CloudWatch 日志来跟踪 DevOps Guru 发送到的请求。 AWS KMS

创建客户托管密钥

您可以使用 AWS 管理控制台 或创建对称的客户托管密钥。 AWS KMS APIs

如要创建对称的客户托管密钥，请参阅创建对称加密 KMS 密钥。

密钥策略

密钥策略控制对客户自主管理型密钥的访问。每个客户托管式密钥必须只有一个密钥策略，其中包含确定谁可以使用密钥以及如何使用密钥的声明。创建客户托管式密钥时，可以指定密钥策略。有关更多信息，请参阅《 AWS Key Management Service 开发人员指南》 AWS KMS中的身份验证和访问控制。

要将您的客户托管密钥与您的 DevOps Guru 资源一起使用，密钥策略中必须允许以下 API 操作：

- `kms:CreateGrant`：向客户托管密钥添加授权。授予对指定 AWS KMS 密钥的控制访问权限，从而允许访问授予 DevOps Guru 所需的操作。有关使用授权的更多信息，请参阅《 AWS Key Management Service 开发者指南》。

这允许 DevOps Guru 执行以下操作：

- 调 GenerateDataKey 用生成加密的数据密钥并将其存储，因为数据密钥不会立即用于加密。
- 调用 Decrypt 使用存储的加密数据密钥访问加密数据。
- 设置停用主体，以允许服务 RetireGrant。
- 用于 kms:DescribeKey 提供客户托管的密钥详细信息，以便 DevOps Guru 验证密钥。

以下声明包括您可以为 DevOps Guru 添加的策略声明示例：

```
"Statement" : [
  {
```

```
      "Sid" : "Allow access to principals authorized to use DevOps Guru",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "*"
      },
      "Action" : [
        "kms:DescribeKey",
        "kms:CreateGrant"
      ],
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "kms:ViaService" : "devops-guru.Region.amazonaws.com",
          "kms:CallerAccount" : "111122223333"
        }
    },
    {
      "Sid": "Allow access for key administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
       },
      "Action" : [
        "kms:*"
       ],
      "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
    },
    {
      "Sid" : "Allow read-only access to key metadata to the account",
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "arn:aws:iam::111122223333:root"
      },
      "Action" : [
        "kms:Describe*",
        "kms:Get*",
        "kms:List*"
      ],
      "Resource" : "*"
    }
  ]
```

流量隐私

您可以将 DevOps Guru 配置为使用接口 VPC 终端节点，从而提高资源分析和见解生成的安全性。为此，您无需互联网网关、NAT 设备或虚拟私有网关。尽管建议这样做 PrivateLink，但也无需进行配置。有关更多信息，请参阅 DevOpsGuru 和接口 VPC 终端节点 ()AWS PrivateLink。有关PrivateLink 和 VPC 终端节点的更多信息，请参阅AWS PrivateLink和通过访问 AWS 服务 PrivateLink。

Amazon DevOps Guru 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 DevOps Guru 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- DevOpsGuru 更新了托 AWS 管策略和服务相关角色
- Amazon DevOps Guru 如何与 IAM 合作
- Amazon Guru 基于身份的政策 DevOps
- 为 DevOps Guru 使用服务相关角色
- Amazon DevOps Guru 权限参考
- Amazon SNS 主题的权限
- AWS KMS已加密的 Amazon SNS 主题的权限
- 对 Amazon DevOps Guru 的身份和访问进行故障排除

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅对 Amazon DevOps Guru 的身份和访问进行故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅Amazon DevOps Guru 如何与 IAM 合作）

- IAM 管理员：编写用于管理访问权限的策略（请参阅Amazon Guru 基于身份的政策 DevOps）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能 AWS 服务 使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中指定主体。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

DevOpsGuru 更新了托 AWS 管策略和服务相关角色

查看自该服务开始跟踪这些更改以来， DevOpsGuru 的 AWS 托管策略和服务相关角色更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 DevOps Guru Amazon DevOps Guru 文档历史记录上的 RSS 提要。

更改	描述	日期
AmazonDevOpsGuruConsoleFullAccess – 对现有策略的更新。	`AmazonDevOpsGuruFullAccess` 托管策略现在支持 Amazon SNS 订阅。	2023 年 8 月 9 日
AmazonDevOpsGuruReadOnlyAccess：对现有策略的更新	`AmazonDevOpsGuruReadOnlyAccess` 托管策略现在支持对 Amazon SNS 订阅列表进行只读访问。	2023 年 8 月 9 日

更改	描述	日期
AmazonDevOpsGuruServiceRolePolicy – 对现有策略的更新。	AWSServiceRoleForDevOpsGuru 服务相关角色现在支持在 RES APIs T 上访问 API Gateway GET 操作。	2023 年 1 月 11 日
AmazonDevOpsGuruServiceRolePolicy – 对现有策略的更新。	AWSServiceRoleForDevOpsGuru 服务相关角色现在支持多个 Amazon Simple Storage Service 和服务限额操作。	2022 年 10 月 19 日
AmazonDevOpsGuruFullAccess：对现有策略的更新	AmazonDevOpsGuruFullAccess 托管策略 现在支持访问该 CloudWatch FilterLogEvents 操作。	2022 年 8 月 30 日
AmazonDevOpsGuruConsoleFullAccess：对现有策略的更新	AmazonDevOpsGuruConsoleFullAccess 托管策略现在支持访问 CloudWatchFilterLogEvents 操作。	2022 年 8 月 30 日
AmazonDevOpsGuruReadOnlyAccess：对现有策略的更新	AmazonDevOpsGuruReadOnlyAccess 托管策略现在支持对该 CloudWatch FilterLogEvents 操作的只读访问权限。	2022 年 8 月 30 日
AmazonDevOpsGuruServiceRolePolicy – 对现有策略的更新。	AWSServiceRoleForDevOpsGuru 服务相关角色现在支持 CloudWatch 日志操作FilterLogEvents DescribeLogGroups 、和。DescribeLogStreams	2022 年 7 月 12 日

更改	描述	日期
DevOpsGuru 基于身份的策略- 新的托管策略。	已添加 AmazonDevOpsGuruConsoleFullAccess 策略。	2021 年 12 月 16 日
AmazonDevOpsGuruServiceRolePolicy – 对现有策略的更新。	AWSServiceRoleForDevOpsGuru 服务相关角色现在支持 Performance Insights DescribeMetricsKeys 和 Amazon RDS DescribeDBInstances 操作。	2021 年 12 月 1 日
AmazonDevOpsGuruReadOnlyAccess：对现有策略的更新	AmazonDevOpsGuruReadOnlyAccess 托管策略现在支持 Amazon RDS DescribeDBInstances 操作的只读访问权限。	2021 年 12 月 1 日
AmazonDevOpsGuruFullAccess：对现有策略的更新	AmazonDevOpsGuruFullAccess 托管策略现在支持访问 Amazon RDS DescribeDBInstances 操作。	2021 年 12 月 1 日

更改	描述	日期
Amazon Guru 基于身份的政策 DevOps – 添加了新策略。	`AWSServiceRoleForDevOpsGuru` 服务相关角色现在支持访问 Amazon RDS `DescribeDBInstances` 和 Performance Insights `GetResourceMetrics` 操作。 `AmazonDevOpsGuruOrganizationsAccess` 托管策略提供对组织内的 DevOps Guru 的访问权限。	2021 年 11 月 16 日
AmazonDevOpsGuruServiceRolePolicy – 对现有策略的更新。	`AWSServiceRoleForDevOpsGuru` 服务相关角色现在支持 AWS Organizations。	2021 年 11 月 4 日
AmazonDevOpsGuruServiceRolePolicy – 对现有策略的更新。	`AWSServiceRoleForDevOpsGuru` 服务相关角色现在包含有关 `ssm:CreateOpsItem` 和 `ssm:AddTagsToResource` 操作的新条件。	2021 年 10 月 11 日
Guru 的服务相关角色权限 DevOps – 对现有策略的更新。	`AWSServiceRoleForDevOpsGuru` 服务相关角色现在包含有关 `ssm:CreateOpsItem` 和 `ssm:AddTagsToResource` 操作的新条件。	2021 年 6 月 14 日

更改	描述	日期
AmazonDevOpsGuruReadOnlyAccess：对现有策略的更新	AmazonDevOpsGuruReadOnlyAccess 托管策略现在允许对 AWS Identity and Access Management GetRole和 DevOps Guru DescribeFeedback 操作进行只读访问。	2021 年 6 月 14 日
AmazonDevOpsGuruReadOnlyAccess：对现有策略的更新	AmazonDevOpsGuruReadOnlyAccess 托管策略现在允许对 DevOps Guru GetCostEstimation 和StartCostEstimation 操作进行只读访问。	2021 年 4 月 27 日
AmazonDevOpsGuruServiceRolePolicy – 对现有策略的更新。	该AWSServiceRoleForDevOpsGuru 角色现在允许访问 AWS Systems Manager AddTagsToResource 和 Amazon EC2 Auto Scaling DescribeAutoScalingGroups 操作。	2021 年 4 月 27 日
DevOpsGuru 开始跟踪更改	DevOpsGuru 开始跟踪其 AWS 托管策略的更改。	2020 年 12 月 10 日

Amazon DevOps Guru 如何与 IAM 合作

在使用 IAM 管理对 DevOps Guru 的访问权限之前，请先了解有哪些 IAM 功能可用于 DevOps Guru。

您可以在 Amazon DevOps Guru 上使用的 IAM 功能

IAM 功能	DevOps大师支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
ACLs	否
ABAC（策略中的标签）	否
临时凭证	是
主体权限	是
服务角色	否
服务关联角色	是

要全面了解 DevOps Guru 和其他 AWS 服务如何使用大多数 IAM 功能，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

Guru 基于身份的政策 DevOps

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Guru 基于身份的策略示例 DevOps

要查看 DevOps Guru 基于身份的策略示例，请参阅。Amazon Guru 基于身份的政策 DevOps

Guru 内部 DevOps基于资源的政策

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

DevOpsGuru 的政策行动

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

要查看 DevOps Guru 操作列表，请参阅《服务授权参考》中的 Amazon DevOps Guru 定义的操作。

DevOpsGuru 中的策略操作在操作前使用以下前缀：

```
aws
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "aws:action1",
      "aws:action2"
         ]
```

要查看 DevOps Guru 基于身份的策略示例，请参阅。Amazon Guru 基于身份的政策 DevOps

DevOpsGuru 的政策资源

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 DevOps Guru 资源类型及其列表 ARNs，请参阅《服务授权参考》中的 Amazon DevOps Guru 定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 A ma DevOps zon Guru 定义的操作。

要查看 DevOps Guru 基于身份的策略示例，请参阅。Amazon Guru 基于身份的政策 DevOps

DevOpsGuru 的策略条件密钥

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Condition` 元素根据定义的条件指定语句何时执行。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 DevOps Guru 条件密钥列表，请参阅《服务授权参考》中的 Amazon DevOps Guru 条件密钥。要了解您可以使用条件键的操作和资源，请参阅 Amazon DevOps Guru 定义的操作。

要查看 DevOps Guru 基于身份的策略示例，请参阅。Amazon Guru 基于身份的政策 DevOps

DevOpsGuru 中的访问控制列表 (ACLs)

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

使用 Guru 进行基于属性的访问控制 (ABAC) DevOps

支持 ABAC（策略中的标签）：否

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`aws:RequestTag/*key-name* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在 DevOps Guru 中使用临时证书

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

Guru 的跨服务主体 DevOps权限

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

DevOpsGuru 的服务角色

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 DevOps Guru 的功能。只有在 DevOps Guru 提供指导时才编辑服务角色。

Guru 的 DevOps服务相关角色

支持服务关联角色：是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

Amazon Guru 基于身份的政策 DevOps

默认情况下，用户和角色无权创建或修改 DevOps Guru 资源。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 DevOps Guru 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》中的 Amazon DevOps Guru 的操作、资源和条件密钥。 ARNs

主题

- 策略最佳实践
- 使用 DevOps Guru 控制台
- 允许用户查看他们自己的权限
- 适用于 DevOps Guru 的 AWS 托管（预定义）策略

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 DevOps Guru资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 DevOps Guru 控制台

要访问 Amazon DevOps Guru 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 AWS 账户的 DevOps Guru 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 DevOps Guru 控制台，还要将 DevOps Guru `AmazonDevOpsGuruReadOnlyAccess` 或`AmazonDevOpsGuruFullAccess` AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

适用于 DevOps Guru 的 AWS 托管（预定义）策略

AWS 通过提供由创建和管理的独立 IAM 策略来解决许多常见用例 AWS。这些 AWS托管策略为常见用例授予必要的权限，因此您可以不必调查需要哪些权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略。

要创建和管理 DevOps Guru 服务角色，还必须附加名为的 AWS托管策略。`IAMFullAccess`

您还可以创建自己的自定义 IAM 策略，以授予 DevOps Guru 操作和资源的权限。您可以将这些自定义策略附加到需要这些权限的用户或组。

以下 AWS托管策略仅适用于 DevOps Guru，您可以将其附加到账户中的用户。

主题

- AmazonDevOpsGuruFullAccess
- AmazonDevOpsGuruConsoleFullAccess
- AmazonDevOpsGuruReadOnlyAccess
- AmazonDevOpsGuruOrganizationsAccess

AmazonDevOpsGuruFullAccess

AmazonDevOpsGuruFullAccess— 提供对 DevOps Guru 的完全访问权限，包括创建 Amazon SNS 主题、访问 CloudWatch 亚马逊指标和 AWS CloudFormation 访问堆栈的权限。仅适用于您想要授予对 Guru 完全控制权的管理员级别用户。 DevOps

AmazonDevOpsGuruFullAccess 策略包含以下语句。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
```

```
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
```

```
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruConsoleFullAccess

AmazonDevOpsGuruConsoleFullAccess— 提供对 DevOps Guru 的完全访问权限，包括创建 Amazon SNS 主题、访问 CloudWatch亚马逊指标和 AWS CloudFormation 访问堆栈的权限。此策略具有额外的性能见解权限，因此您可以在控制台中查看与异常 Amazon RDS Aurora 数据库实例相关的详细分析。仅适用于您想要授予对 Guru 完全控制权的管理员级别用户。 DevOps

AmazonDevOpsGuruConsoleFullAccess 策略包含以下语句。

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruFullAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "SnsTopicOperations",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes",
                "sns:SetTopicAttributes",
                "sns:Subscribe",
```

```
                "sns:Publish"
            ],
            "Resource": "arn:aws:sns:*:*:DevOps-Guru-*"
        },
        {
            "Sid": "DevOpsGuruSlrCreation",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "devops-guru.amazonaws.com"
                }
            }
        },
        {
            "Sid": "DevOpsGuruSlrDeletion",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteServiceLinkedRole",
                "iam:GetServiceLinkedRoleDeletionStatus"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PerformanceInsightsMetricsDataAccess",
            "Effect": "Allow",
            "Action": [
                "pi:GetResourceMetrics",
                "pi:DescribeDimensionKeys"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "CloudWatchLogsFilterLogEventsAccess",
            "Effect": "Allow",
            "Action": [
                "logs:FilterLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/DevOps-Guru-Analysis": "true"
                }
            }
        }
    ]
}
```

AmazonDevOpsGuruReadOnlyAccess

AmazonDevOpsGuruReadOnlyAccess— 授予对 DevOps Guru 和其他 AWS 服务中相关资源的只读访问权限。将此政策应用于您希望授予其查看见解的权限，但不允许其对 DevOps Guru 的分析覆盖范围、Amazon SNS 主题或 System OpsCenter s Manager 集成进行任何更新的用户。

AmazonDevOpsGuruReadOnlyAccess 策略包含以下语句。

JSON

```
    {
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "DevOpsGuruReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "devops-guru:DescribeAccountHealth",
                "devops-guru:DescribeAccountOverview",
                "devops-guru:DescribeAnomaly",
                "devops-guru:DescribeEventSourcesConfig",
                "devops-guru:DescribeFeedback",
                "devops-guru:DescribeInsight",
                "devops-guru:DescribeResourceCollectionHealth",
                "devops-guru:DescribeServiceIntegration",
                "devops-guru:GetCostEstimation",
```

```
                "devops-guru:GetResourceCollection",
                "devops-guru:ListAnomaliesForInsight",
                "devops-guru:ListEvents",
                "devops-guru:ListInsights",
                "devops-guru:ListAnomalousLogGroups",
                "devops-guru:ListMonitoredResources",
                "devops-guru:ListNotificationChannels",
                "devops-guru:ListRecommendations",
                "devops-guru:SearchInsights",
                "devops-guru:StartCostEstimation"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CloudFormationListStacksAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/devops-
guru.amazonaws.com/AWSServiceRoleForDevOpsGuru"
        },
        {
            "Sid": "CloudWatchGetMetricDataAccess",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RDSDescribeDBInstancesAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBInstances"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "SnsListTopicsAccess",
            "Effect": "Allow",
            "Action": [
                "sns:ListTopics",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        },
        {
          "Sid": "CloudWatchLogsFilterLogEventsAccess",
          "Effect": "Allow",
          "Action": [
              "logs:FilterLogEvents"
          ],
          "Resource": "arn:aws:logs:*:*:log-group:*",
          "Condition": {
              "StringEquals": {
                  "aws:ResourceTag/DevOps-Guru-Analysis": "true"
              }
          }
        }
    ]
}
```

AmazonDevOpsGuruOrganizationsAccess

`AmazonDevOpsGuruOrganizationsAccess`— 让 Organizations 管理员可以访问组织内的 DevOps Guru 多账户视图。将此策略应用于您组织的管理员级别用户，您要向其授予组织内的 DevOps Guru 完全访问权限。您可以将此策略应用于您组织的管理账户和 DevOps Guru 的委托管理员帐户。您可以应用`AmazonDevOpsGuruReadOnlyAccess`或`AmazonDevOpsGuruFullAccess`补充本政策，为 DevOps Guru 提供只读或完全访问权限。

`AmazonDevOpsGuruOrganizationsAccess` 策略包含以下语句。

为 DevOps Guru 使用服务相关角色

Amazon DevOps Guru 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接与 DevOps Guru 关联。服务相关角色由 DevOps Guru 预定义，包括

该服务代表您调用 A AWS CloudTrail mazon CloudWatch、 AWS CodeDeploy AWS X-Ray、和 AWS Organizations 所需的所有权限。

与服务相关的角色可以更轻松地设置 DevOps Guru，因为您不必手动添加必要的权限。 DevOpsGuru 定义了其服务相关角色的权限，除非另有定义，否则只有 DevOps Guru 可以担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

只有在首先删除服务相关角色的相关资源后，才能删除该角色。这样可以保护您的 DevOps Guru 资源，因为您不会无意中移除对资源的访问权限。

Guru 的服务相关角色权限 DevOps

DevOpsGuru 使用名为的服务相关角色。AWSServiceRoleForDevOpsGuru这是一项 AWS 托管策略，具有 DevOps Guru 需要在您的账户中运行的限定权限。

AWSServiceRoleForDevOpsGuru 服务相关角色仅信任以下服务来担任该角色：

- devops-guru.amazonaws.com

角色权限策略AmazonDevOpsGuruServiceRolePolicy允许 DevOps Guru 对指定资源完成以下操作。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "cloudtrail:LookupEvents",
    "cloudwatch:GetMetricData",
    "cloudwatch:ListMetrics",
    "cloudwatch:DescribeAnomalyDetectors",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:ListDashboards",
    "cloudwatch:GetDashboard",
    "cloudformation:GetTemplate",
    "cloudformation:ListStacks",
    "cloudformation:ListStackResources",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListImports",
        "codedeploy:BatchGetDeployments",
        "codedeploy:GetDeploymentGroup",
        "codedeploy:ListDeployments",
        "config:DescribeConfigurationRecorderStatus",
        "config:GetResourceConfigHistory",
        "events:ListRuleNamesByTarget",
        "xray:GetServiceGraph",
        "organizations:ListRoots",
        "organizations:ListChildren",
        "organizations:ListDelegatedAdministrators",
        "pi:GetResourceMetrics",
        "tag:GetResources",
        "lambda:GetFunction",
        "lambda:GetFunctionConcurrency",
        "lambda:GetAccountSettings",
        "lambda:ListProvisionedConcurrencyConfigs",
        "lambda:ListAliases",
        "lambda:ListEventSourceMappings",
        "lambda:GetPolicy",
        "ec2:DescribeSubnets",
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:DescribeScalingPolicies",
        "sqs:GetQueueAttributes",
        "kinesis:DescribeStream",
        "kinesis:DescribeLimits",
        "dynamodb:DescribeTable",
        "dynamodb:DescribeLimits",
        "dynamodb:DescribeContinuousBackups",
        "dynamodb:DescribeStream",
        "dynamodb:ListStreams",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "rds:DescribeDBInstances",
        "rds:DescribeDBClusters",
        "rds:DescribeOptionGroups",
        "rds:DescribeDBClusterParameters",
        "rds:DescribeDBInstanceAutomatedBackups",
        "rds:DescribeAccountAttributes",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "s3:GetBucketNotification",
        "s3:GetBucketPolicy",
```

```
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketTagging",
    "s3:GetBucketWebsite",
    "s3:GetIntelligentTieringConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:ListAllMyBuckets",
    "s3:ListStorageLensConfigurations",
    "servicequotas:GetServiceQuota",
    "servicequotas:ListRequestedServiceQuotaChangeHistory",
    "servicequotas:ListServiceQuotas"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowPutTargetsOnASpecificRule",
   "Effect": "Allow",
   "Action": [
    "events:PutTargets",
    "events:PutRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOps-Guru-managed-*"
  },
  {
   "Sid": "AllowCreateOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:CreateOpsItem"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAddTagsToOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:AddTagsToResource"
   ],
   "Resource": "arn:aws:ssm:*:*:opsitem/*"
  },
  {
   "Sid": "AllowAccessOpsItem",
   "Effect": "Allow",
   "Action": [
    "ssm:GetOpsItem",
```

```
    "ssm:UpdateOpsItem"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/DevOps-GuruInsightSsmOpsItemRelated": "true"
    }
   }
  },
  {
   "Sid": "AllowCreateManagedRule",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
  },
  {
   "Sid": "AllowAccessManagedRule",
   "Effect": "Allow",
   "Action": [
    "events:DescribeRule",
    "events:ListTargetsByRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*"
  },
  {
   "Sid": "AllowOtherOperationsOnManagedRule",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/DevOpsGuruManagedRule*",
   "Condition": {
    "StringEquals": {
     "events:ManagedBy": "devops-guru.amazonaws.com"
    }
   }
  },
  {
   "Sid": "AllowTagBasedFilterLogEvents",
   "Effect": "Allow",
```

```
    "Action": [
     "logs:FilterLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/DevOps-Guru-Analysis": "true"
     }
    }
   },
   {
    "Sid": "AllowAPIGatewayGetIntegrations",
    "Effect": "Allow",
    "Action": "apigateway:GET",
    "Resource": [
     "arn:aws:apigateway:*::/restapis/??????????",
     "arn:aws:apigateway:*::/restapis/*/resources",
     "arn:aws:apigateway:*::/restapis/*/resources/*/methods/*/integration"
    ]
   }
  ]
}
```

为 Guru 创建服务相关角色 DevOps

您无需手动创建服务关联角色。当你在 AWS 管理控制台、或 AWS API 中创建见解时 AWS CLI，DevOpsGuru 会为你创建服务相关角色。

> **Important**
>
> 如果您在使用该角色支持的功能的其他服务中完成了操作，则该服务相关角色可能会出现在您的账户中；例如，如果您将 DevOps Guru 添加到存储库中，则该角色可能会出现在您的账户中。 AWS CodeCommit

编辑 Guru 的服务相关角色 DevOps

DevOpsGuru 不允许您编辑`AWSServiceRoleForDevOpsGuru`服务相关角色。创建服务关联角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除 Guru 的服务相关角色 DevOps

如果不再需要使用某个需要服务关联角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，您必须先取消与所有存储库的关联，然后才能手动删除。

> **Note**
>
> 如果您尝试删除资源时 DevOps Guru 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

使用 IAM 手动删除服务关联角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除AWSServiceRoleForDevOpsGuru服务相关角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

Amazon DevOps Guru 权限参考

您可以在 DevOps Guru 策略中使用 AWS宽条件键来表达条件。有关列表，请参阅 IAM 用户指南中的 IAM JSON 策略元素参考。

请在策略的 `Action` 字段中指定这些操作。要指定操作，请在 API 操作名称之前使用 `devops-guru:` 前缀（例如，`devops-guru:SearchInsights` 和 `devops-guru:ListAnomalies`）。要在单个语句中指定多项操作，请使用逗号将它们隔开（例如，`"Action": [ "devops-guru:SearchInsights", "devops-guru:ListAnomalies" ]`）。

使用通配符

您可以在策略的 `Resource` 字段中指定带或不带通配符 (*) 的 Amazon 资源名称（ARN）作为资源值。您可以使用通配符指定多个操作或资源。例如，`devops-guru:*`指定所有 DevOps Guru 操作并`devops-guru:List*`指定所有以单词开头的 DevOps Guru 动作。`List`以下示例涉及以特定 12345 开始的具有通用唯一标识符（UUID）的所有见解。

```
arn:aws:devops-guru:us-east-2:123456789012:insight:12345*
```

在设置 使用身份进行身份验证 和编写您可挂载到 IAM 身份的权限策略（基于身份的策略）时，可以使用下表作为参考。

DevOpsGuru API 操作和操作所需的权限

`AddNotificationChannel`

操作：`devops-guru:AddNotificationChannel`

需要添加来自 DevOps Guru 的通知渠道。当 DevOps Guru 生成包含有关如何改进运营的信息的见解时，通知渠道用于通知您。

资源：*

`RemoveNotificationChannel`

`devops-guru:RemoveNotificationChannel`

需要从 DevOps Guru 中移除通知频道。当 DevOps Guru 生成包含有关如何改进运营的信息的见解时，通知渠道用于通知您。

资源：*

`ListNotificationChannels`

操作：`devops-guru:ListNotificationChannels`

返回为 DevOps Guru 配置的通知渠道列表所必需的。当 DevOps Guru 生成包含如何改进运营信息的见解时，每个通知渠道都用于通知您。支持的一种通知类型是 Amazon Simple Notification Service。

资源：*

`UpdateResourceCollectionFilter`

操作：`devops-guru:UpdateResourceCollectionFilter`

需要更新堆栈列表，这些 CloudFormation 堆栈用于指定 DevOps Guru 分析您账户中的哪些 AWS 资源。该分析会生成包括建议、操作指标和操作事件在内的见解，您可以使用这些见解来提高操作性能。此方法还会创建您使用所需的 IAM 角色 CodeGuru OpsAdvisor。

资源：*

`GetResourceCollectionFilter`

操作：`devops-guru:GetResourceCollectionFilter`

需要返回堆栈列表，这些 AWS CloudFormation 堆栈用于指定 DevOps Guru 分析您账户中的哪些 AWS 资源。该分析会生成包括建议、操作指标和操作事件在内的见解，您可以使用这些见解来提高操作性能。

资源：*

ListInsights

操作：devops-guru:ListInsights

需要在您的 AWS 账户中返回见解列表。您可以按照开始时间、状态（ongoing 或 any）和类型（reactive 或 predictive）指定返回哪些见解。

资源：*

DescribeInsight

操作：devops-guru:DescribeInsight

必须返回有关您使用 ID 指定的见解的详细信息。

资源：*

SearchInsights

操作：devops-guru:SearchInsights

需要在您的 AWS 账户中返回见解列表。您可以按照开始时间、筛选条件和类型（reactive 或 predictive）指定返回哪些见解。

资源：*

ListAnomalies

操作：devops-guru:ListAnomalies

必须返回属于您使用 ID 指定的见解的异常列表。

资源：*

DescribeAnomaly

操作：devops-guru:DescribeAnomaly

必须返回有关您使用 ID 指定的异常的详细信息。

资源：*

ListEvents

操作：devops-guru:ListEvents

需要返回由 DevOps Guru 评估的资源发出的事件列表。您可以使用筛选条件来指定返回哪些事件。

资源：*

ListRecommendations

操作：devops-guru:ListRecommendations

必须返回指定见解的推荐列表。每项建议都包括指标列表和与建议相关的事件列表。

资源：*

DescribeAccountHealth

操作：devops-guru:DescribeAccountHealth

需要返回您的 AWS 账户中已打开的反应式见解的数量、开放的预测见解数量和分析的指标数量。使用这些数字来衡量您 AWS 账户中的运营状况。

资源：*

DescribeAccountOverview

操作：devops-guru:DescribeAccountOverview

必须返回在某个时间范围内发生的以下内容：创建的开放式被动见解的数量、创建的开放式预测性见解的数量，以及所有已关闭的被动见解的平均恢复时间 (MTTR)。

资源：*

DescribeResourceCollectionHealthOverview

操作：devops-guru:DescribeResourceCollectionHealthOverview

需要返回 Guru 中指定的每个 CloudFormation 堆栈的所有洞察的开放预测性见解、开放的被动见解的数量和平均恢复时间 (MTTR)。 DevOps

资源：*

DescribeIntegratedService

操作：devops-guru:DescribeIntegratedService

需要返回可与 DevOps Guru 集成的服务的集成状态。可以与 DevOps Guru集成的一项服务是 AWS Systems Manager，它可用于 OpsItem 为每个生成的见解创建一个。

资源：*

UpdateIntegratedServiceConfig

操作：devops-guru:UpdateIntegratedServiceConfig

需要启用或禁用与可与 DevOps Guru 集成的服务的集成。可以与 DevOps Guru 集成的一项服务是 Systems Manager，它可用于 OpsItem 为每个生成的见解创建一个。

资源：*

Amazon SNS 主题的权限

仅当您想要将 Amazon DevOps Guru 配置为向其他账户拥有的 Amazon SNS 主题发送通知时，才使用本主题中的信息。 AWS

要让 DevOps Guru 向其他账户拥有的 Amazon SNS 主题发送通知，您必须在 Amazon SNS 主题中附加一项政策， DevOps授予 Guru 向其发送通知的权限。如果您将 DevOps Guru 配置为向您用 DevOps于 Guru 的同一账户所拥有的 Amazon SNS 主题发送通知， DevOps则 Guru 会为您在主题中添加策略。

在附加策略以配置另一个账户中某个 Amazon SNS 主题的权限后，您可以在 Guru 中添加 Amazon SNS 主题。 DevOps您还可以使用通知通道更新您的 Amazon SNS 政策，使其更加安全。

> **Note**
>
> DevOpsGuru 目前仅支持同一地区的跨账户访问。

主题

- 另一个账户中的 Amazon SNS 主题的配置权限
- 添加另一个账户的 Amazon SNS 主题
- 使用通知通道更新您的 Amazon SNS 政策（推荐）

另一个账户中的 Amazon SNS 主题的配置权限

作为 IAM 角色添加权限

如果您希望在使用 IAM 角色登录后使用另一个账户中的 Amazon SNS 主题，则必须向要使用的 Amazon SNS 主题附加一个策略。如要在使用 IAM 角色时将策略附加到其他账户的 Amazon SNS 主题，您需要对作为 IAM 角色一部分的账户资源拥有以下权限：

- sns: CreateTopic
- sns: GetTopicAttributes

- sns: SetTopicAttributes
- sns:Publish

将以下策略附加到您要使用的 Amazon SNS 主题。对于Resource密钥，*topic-owner-account-id*是主题所有者的账户 ID，*topic-sender-account-id*是设置 DevOps Guru 的用户的账户 ID，*devops-guru-role*是相关个人用户的 IAM 角色。必须用*region-id*（例如us-west-2）和替换相应的值*my-topic-name*。

以 IAM 用户身份添加权限

要以 IAM 用户身份从其他账户使用 Amazon SNS 主题，请将以下策略附加到要使用的 Amazon SNS 主题。对于Resource密钥，*topic-owner-account-id*是主题所有者的账户 ID，*topic-sender-account-id*是设置 DevOps Guru 的用户的账户 ID，*devops-guru-user-name*是涉及的个人 IAM 用户。必须用*region-id*（例如us-west-2）和替换相应的值*my-topic-name*。

> **Note**
>
> 在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

添加另一个账户的 Amazon SNS 主题

在另一个账户中为某个 Amazon SNS 主题配置权限后，您可以将该 Amazon SNS 主题添加到 DevOps 您的 Guru 通知设置中。您可以使用 AWS CLI 或 DevOps Guru 控制台添加 Amazon SNS 主题。

- 使用控制台时，必须选择 “使用 SNS 主题 ARN 指定现有主题” 选项，才能使用其他账户的主题。
- 使用 AWS CLI 操作时 add-notification-channel，必须在NotificationChannelConfig对象TopicArn内指定。

使用控制台添加来自其他账户的 Amazon SNS 主题

1. 打开 Amazon DevOps Guru 控制台，网址为https://console.aws.amazon.com/devops-guru/。
2. 打开导航窗格，选择设置。
3. 前往“通知”部分并选择 “编辑”。

4. 选择添加 SNS 主题。
5. 选择使用 SNS 主题 ARN 指定现有主题。
6. 输入您要使用的 Amazon SNS 主题的 ARN。您应该已经通过为该主题附加策略来配置该主题的权限。
7. （可选）选择通知配置以编辑通知频率设置。
8. 选择保存。

将 Amazon SNS 主题添加到通知设置后， DevOpsGuru 会使用该主题通知您重要事件，例如创建新见解的时间。

使用通知通道更新您的 Amazon SNS 政策（推荐）

添加主题后，我们建议您仅为包含您的主题的 DevOps Guru 通知渠道指定权限，从而提高策略的安全性。

使用通知通道更新您的 Amazon SNS 主题政策（推荐）

1. 在要从中发送通知的账户中运行 `list-notification-channels` DevOps Guru AWS CLI 命令。

```
aws devops-guru list-notification-channels
```

2. 在 `list-notification-channels` 回复中，记下包含您的 Amazon SNS 主题的 ARN 的通道 ID。通道 ID 是一个指南。

   例如，在以下响应中，带有 ARN `arn:aws:sns:`*region-id*`:`*111122223333*`:`*topic-name* 的主题的通道 ID 为 *e89be5f7-989d-4c4c-b1fe-e7145037e531*

```
{
  "Channels": [
    {
      "Id": "e89be5f7-989d-4c4c-b1fe-e7145037e531",
      "Config": {
      "Sns": {
          "TopicArn": "arn:aws:sns:region-id:111122223333:topic-name"
        },
      "Filters": {
          "MessageTypes": ["CLOSED_INSIGHT", "NEW_INSIGHT", "SEVERITY_UPGRADED"],
          "Severities": ["HIGH", "MEDIUM"]
        }
```

```
      }
    }
  ]
}
```

3. 转到您使用 the section called “另一个账户中的 Amazon SNS 主题的配置权限” 中的主题所有者 ID 在另一个账户中创建的政策。在 Condition 策略声明中，添加指定 SourceArn 的行。ARN 包含您的区域 ID（例如us-east-1）、话题发件人的 AWS 账号以及您记下的频道 ID。

   您的更新的 Condition 声明如下所示。

```
"Condition" : {
  "StringEquals" : {
    "AWS:SourceArn": "arn:aws:devops-guru:us-
east-1:111122223333:channel/e89be5f7-989d-4c4c-b1fe-e7145037e531",
    "AWS:SourceAccount": "111122223333"
   }
 }
```

如果 AddNotificationChannel 无法添加您的 SNS 主题，请检查您的 IAM policy 是否具有以下权限。

AWS KMS已加密的 Amazon SNS 主题的权限

您指定的 Amazon SNS 主题可能由 AWS Key Management Service加密。要允许 DevOps Guru 使用加密主题，您必须先创建一个， AWS KMS key 然后将以下语句添加到 KMS 密钥的策略中。有关更多信息，请参阅使用 AWS KMS、用户指南中的密钥标识符 KeyId () 对发布到 Amazon SNS 的消息进行加密，以及亚马逊简单通知服务开发者指南中的AWS KMS 数据加密。

> **Note**
>
> DevOpsGuru 目前支持在单个账户中使用的加密主题。目前不支持跨多个账户使用加密主题。

对 Amazon DevOps Guru 的身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 DevOps Guru 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 DevOps Guru 中执行任何操作
- 我想为用户提供编程访问权限
- 我无权执行 iam：PassRole
- 我想允许 AWS 账户之外的人访问我的 DevOps Guru 资源

我无权在 DevOps Guru 中执行任何操作

如果 AWS 管理控制台 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。

当 mateojackson 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 aws:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 aws:GetWidget on resource: my-example-widget
```

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 aws:*GetWidget* 操作访问 *my-example-widget* 资源。

我想为用户提供编程访问权限

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS 管理控制台。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

哪个用户需要编程式访问权限？	目的	方式
IAM	（推荐）使用控制台凭证作为临时凭证，签署对 AWS CLI AWS SDKs、或的编程请求 AWS APIs。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》中的“登录 AWS 本地开发”。 • 有关信息 AWS SDKs，请参阅《工具参考指南》AWS SDKs 和《工具参考指南》

哪个用户需要编程式访问权限？	目的	方式
		中的 “登录进行 AWS 本地开发”。
人力身份 （在 IAM Identity Center 中管理的用户）	使用临时证书签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。	按照您希望使用的界面的说明进行操作。 • 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的 “配置 AWS CLI 要使用”。 • 有关工具和 AWS SDKs AWS APIs，请参阅《工具参考指南》中的 IAM 身份中心身份验证AWSSDKs 和工具参考指南。
IAM	使用临时证书签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。	按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。

哪个用户需要编程式访问权限？	目的	方式
IAM	（不推荐使用） 使用长期凭证签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。	按照您希望使用的界面的说明进行操作。 • 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface • 有关 AWS SDKs 和工具，请参阅《工具参考指南》AWS SDKs 和《工具参考指南》中的使用长期凭证进行身份验证。 • 有关信息 AWS APIs，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。

我无权执行 iam：PassRole

如果您收到错误消息，提示您无权执行`iam:PassRole`操作，则必须更新您的策略以允许您将角色传递给 DevOps Guru。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户`marymajor`尝试使用控制台在 DevOps Guru 中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许 AWS 账户之外的人访问我的 DevOps Guru 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 DevOps Guru 是否支持这些功能，请参阅Amazon DevOps Guru 如何与 IAM 合作。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

记录和监控 DevOps Guru

监控是维护 DevOps Guru 和您的其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。AWS 提供以下监控工具，用于监视 DevOps Guru，在出现问题时进行报告，并在适当时自动采取行动：

- Amazon 会实时 CloudWatch监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- AWS CloudTrail捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以标识哪些用户和账户调用了 AWS、发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 AWS CloudTrail 《用户指南》。

主题

- 使用 DevOps Amazon 监控 Guru CloudWatch
- 使用记录 Amazon DevOps Guru API 调用 AWS CloudTrail

使用 DevOps Amazon 监控 Guru CloudWatch

您可以使用监控 DevOps Guru CloudWatch，它会收集原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

对于 DevOps Guru，您可以跟踪指标以获取见解，也可以跟踪您的 DevOps Guru 使用情况的指标。您可能想要密切关注创建的大量 `Insights`，以帮助您确定您的操作解决方案是否存在异常行为。或者，您可能想查看您的 DevOps Guru 使用情况，以帮助跟踪您的成本。

DevOpsGuru 服务在`AWS/DevOps-Guru`命名空间中报告以下指标。

主题

- 见解指标
- DevOpsGuru 使用率指标

见解指标

您可以使用 CloudWatch 跟踪指标，以显示您的 AWS 账户中创建了多少见解。您可以指定 `Type` 维度以跟踪 `proactive` 或 `reactive` 见解。如果您想跟踪所有见解，请不要指定维度。

Metrics

指标	说明
`Insight`	在一个 AWS 账户中创建的见解数量。 有效维度：`Type` 有效统计数据： Sample Count、Sum 单位：计数

DevOpsGuru `Insight` 指标支持以下维度。

Dimensions

维度	说明
Type	这就是见解的类型。如果您想跟踪所有见解，请不要为该 Insights 指标指定维度。有效值为：proactive 、reactive。

DevOpsGuru 使用率指标

您可以使用 CloudWatch 来跟踪您的 Amazon DevOps Guru 使用情况。

Metrics

指标	说明
CallCount	以下 DevOps Guru 方法之一发出的调用次数。 • ListInsights • ListAnomaliesForInsight • ListRecommendations • ListEvents • SearchInsights • DescribeInsight • DescribeAnomaly 有效维度：Service, Class, Type, Resource 有效统计数据： Sample Count、Sum 单位：计数

DevOpsGuru 使用情况指标支持以下维度。

Dimensions

维度	说明
`Service`	包含资源的 AWS 服务的名称。例如，对于 DevOps Guru，此值为`DevOps-Guru` 。
`Class`	这是要跟踪的资源的类别。 DevOpsGuru 将这个维度与值`None`一起使用。
`Type`	这是要跟踪的资源类型。 DevOpsGuru 将这个维度与值`API`一起使用。
`Resource`	这是 DevOps Guru 行动的名称。有效值为：`ListInsights` ，`ListAnomaliesForInsight` ，`ListRecommendations` ，`ListEvents` ，`SearchInsights` ，`DescribeInsight` ，`DescribeAnomaly` 。

使用记录 Amazon DevOps Guru API 调用 AWS CloudTrail

Amazon DevOps Guru 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 DevOps Guru 中执行的操作的记录。 CloudTrail 将 DevOps Guru 的 API 调用捕获为事件。捕获的调用包括来自 DevOps Guru 控制台的调用和对 DevOps Guru API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括 DevOps Guru 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向 DevOps Guru 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail 用户指南。

DevOps大师信息在 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 DevOps Guru 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在自己的 AWS 账户中查看、搜索和下载最近发生的事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您 AWS 账户中的事件，包括 DevOps Guru 的活动，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

DevOpsGuru 支持将其所有操作作为事件记录在 CloudTrail 日志文件中。有关更多信息，请参阅 DevOpsGuru API 参考中的操作。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根凭证还是用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 DevOps Guru 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该`UpdateResourceCollection`操作的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAEXAMPLE:TestSession",
    "arn": "arn:aws:sts::123456789012:assumed-role/TestRole/TestSession",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/TestRole",
        "accountId": "123456789012",
        "userName": "sample-user-name"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-12-03T15:29:51Z"
      }
    }
  },
  "eventTime": "2020-12-01T16:14:31Z",
  "eventSource": "devops-guru.amazonaws.com",
  "eventName": "UpdateResourceCollection",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "sample-ip-address",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.901
 Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.275-b01
 java/1.8.0_275 vendor/Oracle_Corporation",
  "requestParameters": {
    "Action": "REMOVE",
    "ResourceCollection": {
      "CloudFormation": {
        "StackNames": [
          "*"
        ]
      }
    }
  },
  "responseElements": null,
  "requestID": " cb8c167e-EXAMPLE ",
  "eventID": " e3c6f4ce-EXAMPLE ",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012"
}
```

DevOpsGuru 和接口 VPC 终端节点 ()AWS PrivateLink

当您致电 Amazon DevOps Guru APIs 时，您可以使用 VPC 终端节点。当您使用 VPC 端点节点时，您的 API 调用会更加安全，因为它们包含在您的 VPC 中，无法访问互联网。有关更多信息，请参阅 Amazon DevOps Guru API 参考中的操作。

您可以通过创建接口 VPC 终端节点在您的 VPC 和 DevOps Guru 之间建立私有连接。接口终端节点由一项技术提供支持 AWS PrivateLink，该技术使您 APIs 无需互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接即可私密访问 DevOps Guru。您的 VPC 中的实例不需要公有 IP 地址即可与 DevOps Guru APIs 通信。您的 VPC 和 DevOps Guru 之间的流量不会离开亚马逊网络。

每个接口端点均由子网中的一个或多个弹性网络接口表示。

有关更多信息，请参阅 A mazon VPC 用户指南中的接口 VPC 终端节点 (AWS PrivateLink)。

DevOpsGuru VPC 终端节点的注意事项

在为 DevOps Guru 设置接口 VPC 终端节点之前，请务必查看 Amazon VPC 用户指南中的接口终端节点属性和限制。

DevOpsGuru 支持从您的 VPC 调用其所有 API 操作。

为 DevOps Guru 创建接口 VPC 终端节点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为 DevOps Guru 服务创建 VPC 终端节点。有关更多信息，请参阅《Amazon VPC User Guide》中的 Creating an interface endpoint。

使用以下服务名称为 DevOps Guru 创建 VPC 终端节点：

- com.amazonaws。 *region*.devops-guru

例如，如果您为终端节点启用私有 DNS，则可以使用该区域的默认 DNS 名称向 DevOps Guru 发出 API 请求。`devops-guru.us-east-1.amazonaws.com`

有关更多信息，请参阅《Amazon VPC 用户指南》中的通过接口端点访问服务。

为 DevOps Guru 创建 VPC 终端节点策略

您可以将终端节点策略附加到控制对 DevOps Guru 的访问权限的 VPC 终端节点。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

示例： DevOpsGuru 操作的 VPC 终端节点策略

以下是 DevOps Guru 的终端节点策略示例。当连接到终端节点时，此策略会向所有资源的所有委托人授予访问列出的 DevOps Guru 操作的权限。

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "devops-guru:AddNotificationChannel",
            "devops-guru:ListInsights",
            "devops-guru:ListRecommendations"
         ],
         "Resource":"*"
      }
   ]
}
```

DevOpsGuru 的基础设施安全

作为一项托管服务，Amazon DevOps Guru 受到 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 DevOps Guru。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

Amazon DevOps Guru 的韧性

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。 DevOpsGuru 在多个可用区运行，并将工件数据和元数据存储在 Amazon S3 和 Amazon DynamoDB 中。您的加密数据以冗余方式存储在多个设施和每个设施的多个设备中，使其具有高可用性和高持久性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

Amazon DevOps Guru 的配额和限制

下表列出了 Amazon DevOps Guru 中的当前配额。此配额适用于每个 AWS 账户的每个受支持 AWS 区域。

通知

您一次可以指定的 Amazon Simple Notification Service 主题的最大数量	2

CloudFormation 堆栈

您可以指定的最大 AWS CloudFormation 堆栈数	1000

DevOpsGuru 资源监控限制

资源描述	限制	能否增加
监控 Amazon Simple Queue Service (Amazon SQS) 队列的默认限制	100*	是*

*适用于在 2023 年 6 月 29 日当天或之后创建的新 DevOps Guru 账户，以及截至同日处于活跃状态且亚马逊 SQS 队列少于 100 的现有账户。

**要申请更改此限制，请通过 https://aws.amazon.com/contac 支持 t-us联系。您可以请求将 Amazon SQS 队列监控限制设置为 100、500、1,000、5,000 或 10,000。

DevOps创建、部署和管理 API 的大师配额

以下固定配额适用于在 DevOps Guru 中使用 API Gateway 控制台或 API Gateway REST API 及其 SDKs创建、部署和管理 API。 AWS CLI

有关所有 DevOps Guru 的列表 APIs，请参阅 Amazon DevOps Guru 操作。

默认配额	能否增加	
每账户每 1 秒 20 个请求	是	

Amazon DevOps Guru 文档历史记录

下表描述了此版本的 DevOps Guru 的文档。

- API 版本：最新
- 最近文档更新时间：2023 年 8 月 9 日

变更	说明	日期
托管策略更新	Amazon SNS 订阅和订阅列表访问权限已添加到`AmazonDevOpsGuruConsoleFullAccess` 策略。订阅列表访问权限也已添加到`AmazonDevOpsGuruReadOnlyAccess` 策略。有关更多信息，请参阅 Ama DevOps zon Guru 基于身份的政策。	2023 年 8 月 9 日
客户托管的加密键	DevOpsGuru 现在支持使用 AWS KMS客户托管密钥进行加密。有关更多信息，请参阅 DevOpsGuru 中的数据保护。	2023 年 7 月 5 日
DevOpsRDS 版 Guru 支持 RDS PostgreSQL	DevOpsRDS 版 Guru 可以检测 PostgreSQL 数据库中的性能瓶颈和其他见解。有关更多信息，请参阅 RDS 版 DevOps Guru 的好处。	2023 年 3 月 30 日
DevOpsRDS 版 Guru 支持主动见解	DevOpsGuru for RDS 发布了主动见解和建议，以帮助你在 Aurora 数据库中的问题变成更大的问题之前解决这些问题。有关更多信息，请参阅在	2023 年 2 月 28 日

	DevOps Guru for RDS 中处理异常。	
已分析资源页面	DevOpsGuru 控制台中的新页面列出了您账户中由 DevOps Guru 分析的资源。有关更多信息，请参阅查看 DevOps Guru 分析的资源。	2022 年 10 月 20 日
新的通知配置设置	现在，您可以选择是接收所有通知，还是仅接收特定严重程度和事件的通知。有关更多信息，请参阅更新 Amazon SNS 通知配置。	2022 年 9 月 30 日
托管策略中增加了日志异常分析	AWS 已在 IAM 控制台中更新了 DevOps Guru 的托管策略，以支持对该操作的 CloudWatch 访问。`FilterLogEvents` 有关更多信息，请参阅 DevOpsGuru 对 AWS 托管策略和服务相关角色的更新。	2022 年 8 月 30 日
添加了日志异常分析	您可以在 DevOps Guru 控制台中查看与见解相关的日志组的详细信息。还有一个扩展的服务相关角色可用于描述 CloudWatch 日志和流。有关更多信息，请参阅了解 DevOps Guru 控制台中的见解和 DevOps Guru 对 AWS 托管策略和服务相关角色的更新。	2022 年 7 月 12 日

CodeGuru 分析器集成	DevOpsGuru 现在通过 EventBridge 托管规则与 Amazon CodeGuru Profiler 集成。来自 CodeGuru Profiler 的每个入站事件都是一份主动异常报告。有关更多信息，请参阅与 CodeGuru Profiler 集成。	2022 年 3 月 7 日
服务相关角色和托管策略更新	扩展了 IAM 控制台中可用的策略。这些更改使 DevOps Guru 能够支持与亚马逊关系数据库服务（Amazon RDS）的增强集成。有关更多信息，请参阅为 DevOpsG uru 使用服务相关角色和AWS 托管（预定义）策略。	2021 年 12 月 21 日
添加了新的托管策略	`AmazonDevOpsGuruConsoleFullAccess` 策略已添加。有关更多信息，请参阅 Ama DevOps zon Guru 基于身份的政策。	2021 年 12 月 6 日
Support 支持使用 AWS 标签定义应用程序	现在，您可以使用 AWS 标签来识别您希望 DevOps Guru 分析的资源，识别应用程序中的资源，并在控制台中筛选见解。有关更多信息，请参阅使用标签识别应用程序中的资源。	2021 年 12 月 1 日

服务相关角色和托管策略更新	扩展了 IAM 控制台中可用的策略。这些更改使 DevOps Guru 能够支持与亚马逊关系数据库服务（Amazon RDS）的增强集成。有关更多信息，请参阅为 DevOpsG uru 使用服务相关角色和AWS 托管（预定义）策略。	2021 年 12 月 1 日
Amazon RDS 支持	DevOpsGuru 现在为您的应用程序中的亚马逊关系数据库服务 (Amazon RDS) 资源提供全面的分析和见解。有关更多信息，请参阅在 DevOps Guru 中处理适用于 Amazon RDS 的异常。	2021 年 12 月 1 日
亚马逊 EventBridge 集成	DevOpsGuru 现在与集成 EventBridge ，可以通知您与您的 DevOps Guru 见解相关的某些事件。有关更多信息，请参阅使用 EventBridge。	2021 年 11 月 18 日
AWS 已添加托管策略	添加 AWS 了新的托管策略。该`AmazonDevOpsGuruOrganizationsAccess` 策略允许访问组织内的 DevOps Guru。有关更多信息，请参阅基于身份的策略。	2021 年 11 月 16 日
服务相关角色策略更新	扩展了 IAM 控制台中可用的策略。此更改允许 DevOps Guru 支持多账户视图。有关更多信息，请参阅使用服务相关角色。	2021 年 11 月 4 日

跨账户支持	现在，您可以查看组织中多个账户的见解和指标。有关更多信息，请参阅什么是 Amazon DevOps Guru。	2021 年 11 月 4 日
公开发行版本	Amazon DevOps Guru 现已正式上市 (GA)。	2021 年 5 月 4 日
新主题	现在，您可以生成每月成本估算，让 DevOps Guru 分析您的资源。有关更多信息，请参阅估算您的 Amazon DevOps Guru 费用。	2021 年 4 月 27 日
VPC 端点支持	现在，您可以使用 VPC 端点来提高资源分析和见解生成的安全性。有关更多信息，请参阅 DevOpsGuru 和接口 VPC 终端节点 (AWS PrivateLink)。	2021 年 4 月 15 日
新主题	添加了一个关于如何使用 Amazon CloudWatch 监控 DevOps Guru 的新主题。有关更多信息，请参阅使用 Amazon CloudWatch 监控 DevOps Guru。	2020 年 12 月 11 日
预览版	这是 Amazon DevOps Guru 用户指南的预览版。	2020 年 12 月 1 日

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

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。