Amazon Config

开发人员指南

Amazon Config: 开发人员指南

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅中国的 Amazon Web Services 服务入门。

Table of Contents

什么是 Amazon Config？

Amazon Config 可以提供关于您的 Amazon 账户中的 Amazon 资源配置的详细信息。这些信息包括资源之间的关联方式以及资源以前的配置方式，让您了解资源的配置和关系如何随着的时间的推移而更改。

网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的Amazon 资源您可以使用的实体Amazon例如 Amazon Elastic Compute Cloud (EC2) 实例、Amazon Elastic Block Store (EBS) 卷、安全组或 Amazon Virtual Private Cloud (VPC)。有关 Amazon Config 支持的 Amazon 资源的完整列表，请参阅 支持的资源类型 (p. 7)。

利用 Amazon Config，您可以：

- 评估您 Amazon 资源配置是否具备所需设置。
- 获得与您的 Amazon 账户关联的受支持资源的当前配置快照。
- 检索您的账户中的一个或多个资源配置。
- 检索一个或多个资源的历史配置。
- 在资源被创建、修改或删除时接收通知。
- 查看不同资源之间的关系。例如，您可能想要找到使用特定安全组的所有资源。

Amazon Config 的使用方式

当您在 Amazon 上运行应用程序时，您通常要使用 Amazon 资源，这些资源必须共同创建与管理。随着对应用程序的需求的不断增加，记录您的 Amazon 资源的需求也在不断增加。Amazon Config 可以在以下场景中帮助您监督自己的应用程序资源：

资源管理

为了更好地管理您的资源配置并检测资源的错误配置，您需随时详细了解存在哪些资源以及这些资源的配置方式。Amazon Config 可以在资源被创建、修改或删除时向您发送通知，不需要您通过对各个资源进行轮询来监控这些资源更改。

您可以使用 Amazon Config 规则来评估您的 Amazon 资源的配置设置。当 Amazon Config 检测到不符合某项规则中的条件的资源时，Amazon Config 会将其标记为不合规资源并发送通知。Amazon Config 会在您的资源被创建、更改或删除时持续对其进行评估。

审计与合规性

您使用的数据可能需要频繁审计，以确保其符合内部策略与最佳实践。为了证实合规性，您需要了解资源的历史配置。Amazon Config 可以提供这一信息。

对配置更改进行管理与故障排除

当您使用相互依赖的多个 Amazon 资源时，一项资源配置的更改可能对相关资源造成意外后果。利用 Amazon Config，您可以查看您准备修改的资源如何与其他资源相关联，并评估更改所产生的影响。

您也可以使用 Amazon Config 提供的资源历史配置来解决问题，并确定问题资源的最后正确配置。

安全分析

要分析潜在的安全漏洞，您需要有关您的Amazon资源配置，例如Amazon Identity and Access Management 向您的用户授予的 (IAM) 权限或者控制对资源的访问的 Amazon EC2 安全组规则。

您可以使用Amazon Config随时查看 IAM 用户、组或角色的 IAM 策略Amazon Config正在录音。此信息可以帮助您确定用户在特定时间内具备的权限：例如，您可以查看用户是否`John Doe`在 2015 年 1 月 1 日有权修改亚马逊 VPC 设置。

您也可以使用 Amazon Config 来查看您的 EC2 安全组的配置，包括在特定时间打开的端口规则。这一信息可以帮您确定安全组是否会阻止传入 TCP 流量传输至特定端口。

概念

Amazon Config 提供了与您的 Amazon 账户关联的资源的详细视图，包括它们是如何配置的、它们之间是如何相互关联的，以及配置及其关系是如何随时间变化的。让我们详细了解一下 Amazon Config 的概念。

目录

Amazon Config

了解 Amazon Config 的基本组件将帮助您跟踪资源清单以及更改并评估 Amazon 资源的配置。

Amazon 资源

Amazon 资源 是您使用 Amazon Web Services Management Console、Amazon Command Line Interface (CLI)、Amazon 开发工具包或 Amazon 合作伙伴工具创建和管理的实体。的示例Amazon资源包括 Amazon EC2 实例、安全组、Amazon VPC 和亚马逊弹性块存储。Amazon Config用唯一的标识符来引用每个资源，例如资源 ID 或Amazon 资源名称 (ARN). 有关详细信息，请参阅支持的资源类型 (p. 7)。

配置历史

配置历史记录是指定资源在某个时间段的配置项集合。配置历史记录包含多种信息，例如资源首次创建的时间、过去一个月的资源配置情况以及昨天上午 9 点发生了哪些配置更改等。配置历史记录具有多种格式供您使用。Amazon Config将正在记录的各种资源类型的配置历史文件自动传输到您指定的 Amazon S3 存储桶。您可以在 Amazon Config 控制台中选择一项资源，并使用时间线浏览该资源以前的所有配置项。此外，您还可以从 API 访问资源的历史配置项。

配置项

一个配置项代表一个 point-in-time 支持的各种属性的视图Amazon您账户中存在的资源。配置项的组成部分包括元数据、属性、关系、当前配置以及相关事件。只要检测到正在记录的资源类型发生变更，Amazon Config 就会创建配置项。例如，如果Amazon Config正在记录Amazon S3 存储桶，Amazon Config只要创建、更新或删除存储桶，就会创建配置项。

有关更多信息，请参阅 Components of a Configuration Item (p. 24)。

配置记录器

配置记录器以配置项目的形式将受支持资源的配置存储在您的账户中。您必须先创建并启动配置记录器，然后才能开始记录。您可以随时停止或重启配置记录器。有关更多信息，请参阅 管理配置记录器 (p. 79)。

默认情况下，配置记录器会记录 Amazon Config 运行的区域内所有受支持的资源。您可以创建一个自定义配置记录器，仅记录您指定的资源类型。有关更多信息，请参阅 选择 Amazon Config 所记录的资源 (p. 73)。

如果您使用 Amazon Web Services Management Console或 CLI 打开服务，Amazon Config 会自动为您创建并启动一个配置记录器。

配置快照

配置快照是您账户中受支持资源的配置项的集合。配置快照可以完整展示被记录的资源及其配置的相关信息。配置快照是验证您的配置的有效工具。例如，您可以定期检查配置快照，以便找出配置错误的资源或可能不应存在的资源。配置快照具有多种格式。您可以将配置快照传输到您指定的 Amazon SSimple Storage Service (Amazon S3) 存储桶。此外，您可以在 Amazon Config 控制台中选择一个时间点，并按照资源之间的关系浏览不同配置项的快照。

配置流

配置流是一个自动更新的列表，列出了 Amazon Config 正在记录的资源的所有配置项。每当资源被创建、修改或删除时，Amazon Config 会创建一条配置项并将其添加到配置流。配置流在运行时会使用您选择的 Amazon Simple Notification Service (Amazon SNS) 主题。配置流可以帮助您随时观察配置更改，以便发现潜在的问题、在特定资源发生更改时生成通知，或更新需要反映您的 Amazon 资源配置的外部系统。

资源关系

Amazon Config 会查找您账户中的 Amazon 资源，然后创建 Amazon 资源关系图。例如，卷包含 Amazon EBS 卷`vol-123ab45d`附加到 Amazon EC2 实例`i-a1b2c3d4`与安全组关联的`sg-ef678hk`.

有关更多信息，请参阅 支持的资源类型 (p. 7)。

Amazon Config 托管和自定义规则

Amazon Config 规则表示特定 Amazon 资源或整个 Amazon 账户所需的配置设置。Amazon Config 提供可自定义的预定义规则来帮助您入门。如果某个资源违反规则，Amazon Config将资源和规则标记为不合规，并且Amazon Config将通过Amazon SNS 通知您。

Amazon Config 自定义规则

通过 Amazon Config，您还可以创建自定义规则。Amazon Config 会持续跟踪您的资源配置更改，同时检查这些更改是否符合规则中设定的所有条件。

激活一项规则后，Amazon Config 会将您的资源与规则中的条件进行比较。完成这一初始评估后，Amazon Config 会在每次触发评估时继续执行评估。规则中会定义评估触发器，可以包括以下类型：

- 配置更改 —Amazon Config配置更改与规则范围匹配的任何资源时，将触发评估。在 Amazon Config 发送配置项更改通知后，评估便会运行。
- 定期的 —Amazon Config按照您选择的频率运行规则的评估（例如，每 24 小时）。

有关更多信息，请参阅 使用 Amazon Config 规则评估资源 (p. 105)。

管理 Amazon Config

Amazon Config 控制台

您可以使用 Amazon Config 控制台管理服务。此控制台提供了用于执行许多 Amazon Config 任务的用户界面，这些任务包括：

- 为记录指定 Amazon 资源的类型。
- 配置要记录的资源，包括：
  - 选择 Simple Storage Service（Amazon S3）存储桶。
  - 选择Amazon SNS 主题。
  - 创建 Amazon Config 角色。
- 创建表示特定 Amazon 资源或整个 Amazon 账户所需的配置设置的托管规则和自定义规则。
- 创建和管理配置聚合器以跨多个账户和地区聚合数据。
- 查看受支持资源的当前配置的快照。
- 查看 Amazon 资源之间的关系。

有关 Amazon Web Services Management Console 的更多信息，请参阅 Amazon Web Services Management Console。

Amazon Config CLI

Amazon Command Line Interface 是一个可用于从命令行与 Amazon Config 交互的统一工具。有关更多信息，请参阅《Amazon Command Line Interface 用户指南》。有关 Amazon Config CLI 命令的完整列表，请参阅可用命令。

Amazon Config API

除了控制台和 CLI 之外，您还可以使用 Amazon Config RESTful API 来直接对 Amazon Config 进行编程。有关详细信息，请参阅 Amazon Config API 参考。

Amazon 软件开发工具包

作为使用Amazon ConfigAPI，您可以使用其中的一个Amazon软件开发工具包。每个软件开发工具包均包含适用于各种编程语言和平台的库和示例代码。这些开发工具包提供了一种简便方法，以使用编程方式访问Amazon Config。例如，您可以使用开发工具包以加密方式对请求进行签名，管理错误并自动重试请求。有关更多信息，请参阅用于 Amazon Web Services 的工具页面。

控制对 Amazon Config 的访问权限

Amazon Identity and Access Management 是一项 Web 服务，Amazon Web Services (Amazon) 客户可使用此服务管理用户和用户权限。使用 IAM 为需要对 Amazon Config 的访问权的任何人创建单独的用户。为您自己创建一个 IAM 用户，授予该 IAM 用户管理权限，并将该 IAM 用户用于您的所有工作。在为访问您的账户的人员创建单独的 IAM 用户时，您可授予每个 IAM 用户一组独特的安全凭证。您还可向每个 IAM 用户授予不同的权限。如有必要，可以随时更改或撤消 IAM 用户的权限。有关更多信息，请参阅 Amazon Identity and Access Management (p. 216)。

合作伙伴解决方案

Amazon 与日志记录和分析方面的第三方专家协作以提供利用 Amazon Config 输出的解决方案。有关更多信息，请访问Amazon Config详细信息页面位于Amazon Config.

Amazon Config 的工作原理

打开 Amazon Config 之后，它会先查找您账户中受支持的 Amazon 资源，并为每个资源生成一个配置项 (p. 3)。

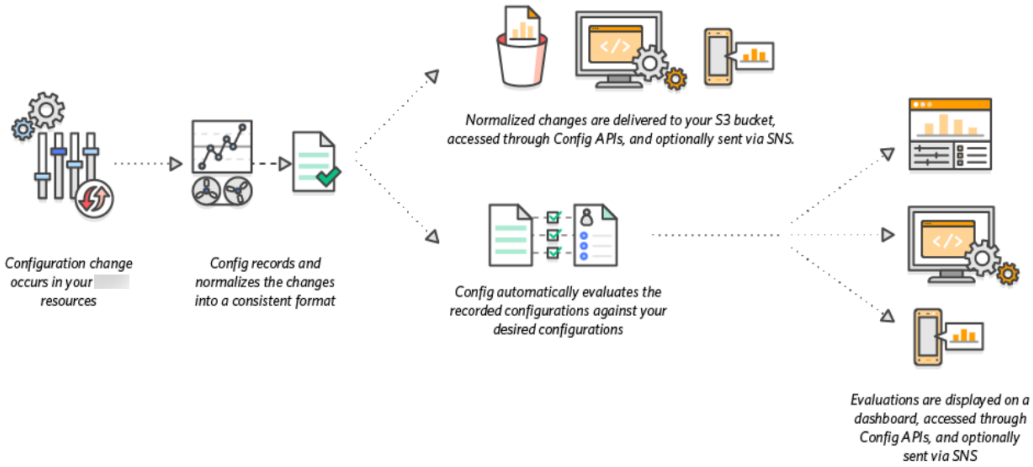
Amazon Config 还会在某个资源的配置更改时生成配置项，并在您启动配置记录器后，保留配置项的历史记录。默认情况下，Amazon Config 会为区域内每个支持的资源创建配置项。如果您不希望 Amazon Config 为所有支持的资源都创建配置项，您可以指定希望其跟踪的资源类型。

Amazon Config 可以针对您账户中的每个资源调用 Describe 或 List API，从而记录您的资源的所有更改。该服务使用相同的 API 调用来捕获所有相关资源的配置详细信息。

例如，从 VPC 安全组删除出站规则将导致 Amazon Config 对安全组调用 Describe API。之后，Amazon Config 会对与该安全组关联的所有实例调用 Describe API。安全组（资源）以及每个实例（相关资源）的更新后配置将被记录为配置项，并以配置流的形式传送到 Amazon Simple Storage Service (Amazon S3) 存储桶。

Amazon Config 还会跟踪不是由 API 发起的配置更改。Amazon Config 会定期检查资源配置，并针对已更改的配置生成配置项。

如果您使用的是 Amazon Config 规则，则 Amazon Config 会持续评估您的 Amazon 资源是否具备所需设置。根据具体规则，Amazon Config 会在配置更改时评估您的资源或定期进行评估。每个规则都与一个 Amazon Lambda 函数关联，其中包含规则的评估逻辑。当 Amazon Config 评估您的资源时，它会调用规则的 Amazon Lambda 函数。该函数会返回被评估资源的合规性状态。如果某个资源不符合某项规则的条件，那么 Amazon Config 会将该资源和规则标记为不合规。当某个资源的合规性状态发生更改时，Amazon Config将通知发送到 Amazon SNS 主题。



传送配置项

Amazon Config 可以通过以下通道传送配置项：

Amazon S3 存储桶

Amazon Config跟踪你的配置中的变化Amazon并将更新后的配置详细信息定期发送到您指定的 Amazon S3 存储桶。对于 Amazon Config 记录的每个资源类型，它会每隔 6 小时发送一个配置历史记录文件。每个配置历史记录文件中都包含前 6 小时内发生更改的资源的详细信息。每个文件均包含一种类型的资源，例如 Amazon EC2 实例或 Amazon EBS 卷。如果配置未发生更改，Amazon Config 则不会发送文件。

Amazon Config发送配置快照当您使用时会转到 Amazon S3 存储桶。deliver-config-snapshot命令使用 AmazonCLI，或者当你使用DeliverConfig快照使用操作Amazon ConfigAPI。配置快照包含 Amazon Config 在您的 Amazon 账户中记录的所有资源的配置详细信息。配置历史记录文件和配置快照均采用 JSON 格式。

> Note
>
> Amazon Config 仅将配置历史记录文件和配置快照传输到指定的 S3 存储桶；Amazon Config 不会修改 S3 存储桶中对象的生命周期策略。您可以使用生命周期策略指定是删除对象还是将对象存档到 Amazon S3 Glacier。有关更多信息，请参阅 。管理生命周期配中的Amazon Simple Storage Service 用户指南. 您还可看到将 Amazon S3 数据存档到 S3 Glacier博客帖子。

Amazon SNS 主题

Amazon Simple Notification Service (Amazon SNS) 主题是 Amazon SNS 用于传送消息（或）的通信渠道。通知) 订阅终端节点，例如电子邮箱地址或客户端。其他类型的 Amazon SNS 通知包括传送到手机应用程序上的推送通知消息、传送到支持短信服务功能的手机上的短信服务 (SMS) 通知以及 HTTP POST 请求。为了获得最佳效果，请使用 Amazon SQS 作为 SNS 主题的通知终端节点，然后以编程方式处理通知中的信息。

Amazon Config使用您指定的 Amazon SNS 主题向您发送通知。您收到的通知的类型由消息正文中的 `messageType` 键的值体现，如以下示例所示：

```
"messageType": "ConfigurationHistoryDeliveryCompleted"
```

通知可以是以下任一类型的消息：

`ComplianceChangeNotification`

Amazon Config 评估的资源的合规性状态已更改。合规性类型指示资源是否符合特定的 Amazon Config 规则，并且它由消息中的 `ComplianceType` 键表示。消息中包含 `newEvaluationResult` 和 `oldEvaluationResult` 对象，以便进行比较。

`ConfigRulesEvaluationStarted`

Amazon Config 开始针对指定的资源评估您的规则。

`ConfigurationSnapshotDeliveryStarted`

Amazon Config已开始将配置快照传送到 Amazon S3 存储桶。提供了 Amazon S3 存储桶的名称。`s3Bucket`键入消息。

`ConfigurationSnapshotDeliveryCompleted`

Amazon Config已成功将配置快照传送到 Amazon S3 存储桶。

`ConfigurationSnapshotDeliveryFailed`

Amazon Config未能将配置快照传送到 Amazon S3 存储桶。

`ConfigurationHistoryDeliveryCompleted`

Amazon Config已成功将配置历史记录传送到 Amazon S3 存储桶。

`ConfigurationItemChangeNotification`

某个资源的已被创建、删除或更改配置。此消息包含 Amazon Config 针对上述更改创建的配置项的详细信息，其中包括更改的类型。上述通知均在发生更改后的几分钟内传送，统称为配置流。

`OversizedConfigurationItemChangeNotification`

当配置项变更通知超出 Amazon SNS 允许的最大大小时会传送此消息类型。消息中包括配置项摘要。除了 SMS 消息外，Amazon SNS 消息最多可包含 256 KB 的文本数据，包括 XML、JSON 和未格式化的文本。您可以在指定的 Amazon S3 存储桶位置查看完整通知。

`OversizedConfigurationItemChangeDeliveryFailed`

Amazon Config未能将过大配置项变更通知传送到 Amazon S3 存储桶。

有关示例通知，请参阅 Amazon Config 发送到 Amazon SNS 主题的通知 (p. 91)。

有关 Amazon SNS 的更多信息，请参阅 Amazon Simple Notification Service 开发人员指南。

支持的资源类型

Amazon Config 支持以下 Amazon 资源类型和资源关系。某些区域只支持其中一部分资源类型。中有哪些可用Amazon Config给定区域中的控制台是关于给定区域支持或不支持哪些内容的真相来源。

的高级查询Amazon Config支持其中一部分资源类型。有关这些受支持的资源类型的列表，请参阅高级查询的Support 资源类型.

Note

定期规则可以在以下资源上运行Amazon Config录制不支持，可以在未启用配置记录器的情况下运行。定期规则不依赖于配置项。有关更改触发规则和周期性规则之间的区别的更多信息，请参阅为指定触发器Amazon ConfigRule.
何时Amazon Config在boards新资源类型中，新资源类型的默认资源将在账户基准设定过程中被发现。如果您已将配置记录器设置为记录所有受支持的资源类型，则在新资源类型正在加载过程中，您可能会收到默认资源的通知。入职流程完成后，将更新公共文档。

Amazon API Gateway

Amazon 服务	资源类型值	关系	相关资源
API Gateway	`AWS::ApiGateway::Stage`	包含在	ApiGateway Rest API
		关联到	WAFRegional WebACL
	`AWS::ApiGatewayV2::Stage`	包含在	ApiGatewayV2 Api
	`AWS::ApiGateway::RestApi`	包含	ApiGateway 阶段
	`AWS::ApiGatewayV2::Api`	包含	ApiGatewayV2 Stage

了解相关更多信息Amazon Config与Amazon API Gateway 相集成使用监控 API Gateway API 配置Amazon Config.

亚马逊 CloudFront

Amazon 服务	资源类型值	关系	相关资源
亚马逊 CloudFront*	`AWS::CloudFront::Distribution`	关联到	AmazonWAF WebACL
			ACM 证书

Amazon 服务	资源类型值	关系	相关资源
			S3Bucket
			IAM 服务器证书
	AWS::CloudFront::StreamingDistribution	关联到	AmazonWAF WebACL
			ACM 证书
			S3Bucket
			IAM 服务器证书

*Amazon Config对Amazon CloudFront 仅在美国东部 (弗吉尼亚北部) 区域提供。

亚马逊 CloudWatch

Amazon 服务	资源类型值	关系	相关资源
亚马逊 CloudWatch	AWS::CloudWatch::Alarm	NA	NA

Amazon DynamoDB

Amazon 服务	资源类型值	关系	相关资源
Amazon DynamoDB	AWS::DynamoDB::Table	NA	NA

Amazon Elastic Block Store

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Block Store	AWS::EC2::Volume	挂载到	EC2 实例

Amazon Elastic Compute Cloud

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Compute Cloud	AWS::EC2::Host*	包含	EC2 实例
	AWS::EC2::EIP	挂载到	EC2 实例
			网络接口
	AWS::EC2::Instance	包含	EC2 网络接口
		关联到	EC2 安全组
		挂载到	Amazon EBS 卷

Amazon 服务	资源类型值	关系	相关资源
			EC2 弹性 IP (EIP)
		包含在	EC2 专用主机
			路由表
			子网
			Virtual Private Cloud (VPC)
	AWS::EC2::NetworkInterface	关联到	EC2 安全组
		挂载到	EC2 弹性 IP (EIP)
			EC2 实例
		包含在	路由表
			子网
			Virtual Private Cloud (VPC)
	AWS::EC2::SecurityGroup	关联到*	EC2 实例
			EC2 网络接口
			Virtual Private Cloud (VPC)
	AWS::EC2::NatGateway	包含在	Virtual Private Cloud (VPC)
		包含在	子网
	AWS::EC2::EgressOnlyInternetGateway	挂载到	Virtual Private Cloud (VPC)
	AWS::EC2::FlowLog	NA	NA
	AWS::EC2::TransitGateway	NA	NA
	AWS::EC2::TransitGatewayAttachment	NA	NA
	AWS::EC2::TransitGatewayRouteTable	NA	NA
	AWS::EC2::VPCEndpoint	包含在	Virtual Private Cloud (VPC)
		挂载到	网络接口
		包含在	子网
		包含在	路由表
	AWS::EC2::VPCEndpointService	关联到	ElasticLoadBalancingV2 LoadBalancer

Amazon 服务	资源类型值	关系	相关资源
	AWS::EC2::VPCPeeringConnection	关联到	Virtual Private Cloud (VPC)
	AWS::EC2::RegisteredHAInstance	关联到	EC2 实例
	AWS::EC2::LaunchTemplate	NA	NA

*Amazon Config 会记录专用主机以及在其上启动的实例的配置详细信息。因此，在报告与服务器绑定的软件许可证的合规情况时，您可以将 Amazon Config 用作数据源。例如，您可以查看某个实例的配置历史记录并确定其基于哪个 Amazon 系统映像 (AMI)。然后，您可以查找相应主机的配置历史记录 (包括套接字和核心数量之类的详细信息)，以验证该主机是否符合 AMI 的许可证要求。有关更多信息，请参阅 。使用 跟踪配置更改Amazon Config中的适用于Linux 实例的 Amazon EC2 用户指南.

*EC2 SecurityGroup 属性定义包含 IP CIDR 块，这些块在内部转换为 IP 范围，在尝试查找特定 IP 范围时可能会返回意外结果。有关搜索特定 IP 范围的解决方法，请参阅对高级查询的限制.

Amazon Elastic Container Registry

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Container Registry	AWS::ECR::Repository	NA	NA

Amazon Elastic Container Registry Public

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Container Registry Public*	AWS::ECR::PublicRepository	NA	NA

*Amazon Config对 Amazon Elastic Contaer Regit Conter Regit Public 的支持仅在美国东部 (弗吉

Amazon Elastic Container Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Container Service	AWS::ECS::Cluster	NA	NA
	AWS::ECS::TaskDefinition	NA	NA
	AWS::ECS::Service*	NA	NA

*此服务目前仅支持新的Amazon Resource Name (ARN) 格式。有关更多信息，请参阅 。Amazon 资源名称 (ARN) 和 ID在 ECS 开发人员指南中。

旧（不支持）：arn:aws:ecs:*region*:*aws_account_id*:service/*service-name*

新（支持）：`arn:aws:ecs:region:aws_account_id:service/cluster-name/service-name`

Amazon Elastic File System

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic File System	`AWS::EFS::FileSystem`	NA	NA
	`AWS::EFS::AccessPoint`	NA	NA

Amazon Elastic Kubernetes Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Kubernetes Service	`AWS::EKS::Cluster`	NA	NA

Amazon EMR

Amazon 服务	资源类型值	关系	相关资源
Amazon EMR	`AWS::EMR::SecurityConfiguration`	NA	NA

亚马逊 GuardDuty

Amazon 服务	资源类型值	关系	相关资源
亚马逊 GuardDuty	`AWS::GuardDuty::Detector`	NA	NA

亚马逊 OpenSearch 服务

Amazon 服务	资源类型值	关系	相关资源
亚马逊 OpenSearch 服务	`AWS::Elasticsearch::Domain`	关联到	KMS 密钥
			EC2 安全组
			EC2 子网
			Virtual Private Cloud (VPC)
	`AWS::OpenSearch::Domain`	NA	NA

Amazon Quantum Ledger Database (Amazon QLDB)

Amazon 服务	资源类型值	关系	相关资源
Amazon QLDB	`AWS::QLDB::Ledger`	NA	NA

Amazon Kinesis

Amazon 服务	资源类型值	关系	相关资源
Amazon Kinesis	`AWS::Kinesis::Stream`	NA	NA
	`AWS::Kinesis::StreamConsumer`	NA	NA

Amazon Managed Streaming for Apache Kafka

Amazon 服务	资源类型值	关系	相关资源
Amazon Managed Streaming for Apache Kafka	`AWS::MSK::Cluster`	NA	NA

Amazon Redshift

Amazon 服务	资源类型值	关系	相关资源
Amazon Redshift	`AWS::Redshift::Cluster`	关联到	集群参数组
			集群安全组
			集群子网组
			安全组
			Virtual Private Cloud (VPC)
	`AWS::Redshift::ClusterParameterGroup`	NA	NA
	`AWS::Redshift::ClusterSecurityGroup`	NA	NA
	`AWS::Redshift::ClusterSnapshot`	关联到	Cluster
			Virtual Private Cloud (VPC)
	`AWS::Redshift::ClusterSubnetGroup`	关联到	子网
			Virtual Private Cloud (VPC)

Amazon 服务	资源类型值	关系	相关资源
	AWS::Redshift::EventSubscription	NA	NA

Amazon Relational Database Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Relational Database Service	AWS::RDS::DBInstance	关联到	EC2 安全组
			RDS 数据库安全组
			RDS 数据库子网组
	AWS::RDS::DBSecurityGroup	关联到	EC2 安全组
			Virtual Private Cloud (VPC)
	AWS::RDS::DBSnapshot	关联到	Virtual Private Cloud (VPC)
	AWS::RDS::DBSubnetGroup	关联到	EC2 安全组
			Virtual Private Cloud (VPC)
	AWS::RDS::EventSubscription	NA	NA
	AWS::RDS::DBCluster	包含	RDS 数据库实例
		关联到	RDS 数据库子网组
			EC2 安全组
	AWS::RDS::DBClusterSnapshot	关联到	RDS 数据库集群
			Virtual Private Cloud (VPC)

Amazon Route 53

Amazon 服务	资源类型值	关系	相关资源
Amazon Route 53	AWS::Route53Resolver::ResolverEndpoint	NA	NA
	AWS::Route53Resolver::ResolverRule	NA	NA
	AWS::Route53Resolver::ResolverRuleAssociation	NA	NA

Amazon S3 存储桶属性

Amazon Config还会记录对于 Amazon S3 存储桶资源类型的 Amazon S3 的以下属性。

属性	描述
AccelerateConfiguration	在您的客户端与存储桶之间远距离传输的数据的传输加速。
BucketAcl	用于管理存储桶和对象访问的访问控制列表。
BucketPolicy	用于定义存储桶权限的策略。
CrossOriginConfiguration	允许跨区域请求存储桶。
LifecycleConfiguration	用于定义您存储桶中的对象生命周期的规则。
LoggingConfiguration	用于跟踪存储桶访问请求的日志记录。
NotificationConfiguration	用于针对指定存储桶事件发送警报或触发工作流的事件通知。
ReplicationConfiguration	在不同 Amazon 区域中的存储桶之间自动以异步方式复制对象。
RequestPaymentConfiguration	启用申请方付款。
TaggingConfiguration	添加到存储桶用于分类的标签。您也可以使用标记或跟踪计费。
WebsiteConfiguration	对存储桶启用静态网站托管。
VersioningConfiguration	对存储桶中的对象启用版本控制。

有关属性的更多信息，请参阅存储桶配置选项中的Amazon Simple Service.

亚马逊 SageMaker

Amazon 服务	资源类型值	关系	相关资源
亚马逊 SageMaker	`AWS::SageMaker::CodeRepository`	NA	NA
	`AWS::SageMaker::Model`	NA	NA
	`AWS::SageMaker::NotebookInstance`	NA	NA

Amazon Simple Notification Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Simple Notification Service	`AWS::SNS::Topic`	NA	NA

Amazon Simple Queue Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Simple Queue Service	`AWS::SQS::Queue`	NA	NA

Amazon Simple Storage Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Simple Storage Service	`AWS::S3::Bucket`*	NA	NA
	`AWS::S3::AccountPublicAccessBlock`	NA	NA

*如果您已将 Amazon Config 配置为记录您的 S3 存储桶但未收到配置更改通知，请验证您的 S3 存储桶策略是否拥有必需的权限。有关更多信息，请参阅 管理 S3 存储桶录制权限 (p. 221)。

Amazon Virtual Private Cloud

Amazon 服务	资源类型值	关系	相关资源
Amazon Virtual Private Cloud	`AWS::EC2::CustomerGateway`	挂载到	VPN 连接
	`AWS::EC2::InternetGateway`	挂载到	Virtual Private Cloud (VPC)
	`AWS::EC2::NetworkAcl`	NA	NA
	`AWS::EC2::RouteTable`	包含	EC2 实例
			EC2 网络接口
			子网
			VPN 网关
		包含在	Virtual Private Cloud (VPC)
	`AWS::EC2::Subnet`	包含	EC2 实例
			EC2 网络接口
		挂载到	网络 ACL
		包含在	路由表
			Virtual Private Cloud (VPC)
	`AWS::EC2::VPC`	包含	EC2 实例
			EC2 网络接口
			网络 ACL
			路由表
			子网
		关联到	安全组
		挂载到	Internet 网关

Amazon 服务	资源类型值	关系	相关资源
			VPN 网关
	AWS::EC2::VPNConnection	挂载到	客户网关
			VPN 网关
	AWS::EC2::VPNGateway	挂载到	Virtual Private Cloud (VPC)
			VPN 连接
		包含在	路由表

Amazon Auto Scaling

Amazon 服务	资源类型值	关系	相关资源
Amazon Auto Scaling	AWS::AutoScaling::AutoScalingGroup	包含	Amazon EC2 实例
		关联到	Classic Load Balancer
			Auto Scaling 启动配置
			子网
	AWS::AutoScaling::LaunchConfiguration	关联到	Amazon EC2 安全组
	AWS::AutoScaling::ScalingPolicy	关联到	Auto Scaling 组
			警报
	AWS::AutoScaling::ScheduledAction	关联到	Auto Scaling 组

亚马逊 WorkSpaces

Amazon 服务	资源类型值	关系	相关资源
亚马逊 WorkSpaces	AWS::WorkSpaces::ConnectionAlias	NA	NA
	AWS::WorkSpaces::Workspace	NA	NA

Amazon Backup

Amazon 服务	资源类型值	关系	相关资源
Amazon Backup	AWS::Backup::BackupPlan	NA	NA*
	AWS::Backup::BackupSelection	NA	NA
	AWS::Backup::BackupVault	NA	NA*

Amazon 服务	资源类型值	关系	相关资源
	AWS::Backup::RecoveryPoint	NA	NA

由于如何Amazon Backupworks，其中一些资源类型与其他资源类型相关Amazon Backup此表中的资源类型。

AWS::Backup::BackupPlan与AWS::Backup::BackupSelection其中Backup 计划有很多选择，并且AWS::Backup::BackupVault与AWS::Backup::RecoveryPoint其中，Amazon Backup文件库有多个恢复点。

有关更多信息，请参阅 。使用备份计划管理备份和处理备份文件库.

Amazon Batch

Amazon 服务	资源类型值	关系	相关资源
Amazon Batch	AWS::Batch::JobQueue	NA	NA
	AWS::Batch::ComputeEnvironment	NA	NA

Amazon Certificate Manager

Amazon 服务	资源类型值	关系	相关资源
Amazon Certificate Manager	AWS::ACM::Certificate	NA	NA

Amazon CloudFormation

Amazon 服务	资源类型值	关系	相关资源
Amazon CloudFormation	AWS::CloudFormation::Stack	包含*	支持的 Amazon 资源类型

*Amazon Config 会记录对 Amazon CloudFormation 堆栈和堆栈中支持的资源类型所做的配置更改。Amazon Config 不会记录对堆栈中的尚不受支持的资源类型所做的配置更改。不受支持的资源类型显示在堆栈的配置项的补充配置部分中。

Amazon CloudTrail

Amazon 服务	资源类型值	关系	相关资源
Amazon CloudTrail	AWS::CloudTrail::Trail	NA	NA

Amazon CodeBuild

Amazon 服务	资源类型值	关系	相关资源
Amazon CodeBuild	AWS::CodeBuild::Project	关联到*	S3 存储桶
			IAM 角色

*要了解有关 Amazon Config 如何与 Amazon CodeBuild 集成的更多信息，请参阅将 Amazon Config 与 Amazon CodeBuild 示例配合使用。

Amazon CodeDeploy

Amazon 服务	资源类型值	关系	相关资源
Amazon CodeDeploy	AWS::CodeDeploy::Application	包含	DeploymentGroup
	AWS::CodeDeploy::DeploymentConfig	NA	NA
	AWS::CodeDeploy::DeploymentGroup	包含在	应用程序

Amazon CodePipeline

Amazon 服务	资源类型值	关系	相关资源
Amazon CodePipeline	AWS::CodePipeline::Pipeline	托管到*	S3 存储桶
		关联到	IAM 角色
			代码项目
			Lambda 函数
			Cloudformation 堆栈
			ElasticBeanstalk 应用程序

*Amazon Config将配置更改记录到 CodePipeline 管道和管道中支持的资源类型。Amazon Config不会记录对管道中尚不支持的资源类型所做的配置更改。不受支持的资源类型（如 `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, 和 `ECS service`）显示在堆栈的配置项的补充配置部分中。

Amazon Config

Amazon 服务	资源类型值	关系	相关资源
Amazon Config	AWS::Config::ResourceCompliance	关联到*	所有资源*

Amazon 服务	资源类型值	关系	相关资源
	AWS::Config::ConformancePackCompliance	NA	NA

*两者之间的关系AWS::Config::ResourceCompliance相关资源取决于如何AWS::Config::ResourceCompliance会报告对特定资源类型的合规性。

Note

为录制AWS::Config::ConformancePackCompliance资源类型不另外收取费用。

Amazon Database Migration Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Database Migration Service	AWS::DMS::EventSubscription	NA	NA
	AWS::DMS::ReplicationSubnetGroup	NA	NA

Amazon Elastic Beanstalk

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Beanstalk	AWS::ElasticBeanstalk::Application	包含	Elastic Beanstalk 应用程序版本
			Elastic Beanstalk 环境
		关联到	IAM 角色
	AWS::ElasticBeanstalk::ApplicationVersion	包含在	Elastic Beanstalk 应用程序
		关联到	Elastic Beanstalk 环境
			S3 存储桶
	AWS::ElasticBeanstalk::Environment	包含在	Elastic Beanstalk 应用程序
		关联到	Elastic Beanstalk 应用程序版本
			IAM 角色
		包含	CloudFormation 堆栈

Amazon Global Accelerator

Amazon 服务	资源类型值	关系	相关资源
Amazon Global Accelerator	AWS::GlobalAccelerator::Listener*	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::GlobalAccelerator::EndpointGroup*	NA	NA
	AWS::GlobalAccelerator::Accelerator*	NA	NA

*此资源仅在美国西部（俄勒冈）区域提供。

Amazon Identity and Access Management

Amazon 服务	资源类型值	关系	相关资源
Amazon Identity and Access Management	AWS::IAM::User	挂载到	IAM 组
			IAM 客户托管策略
	AWS::IAM::Group	包含	IAM 用户
		挂载到	IAM 客户托管策略
	AWS::IAM::Role	挂载到	IAM 客户托管策略
	AWS::IAM::Policy	挂载到	IAM 用户
			IAM 组
			IAM 角色
Amazon Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	NA	NA

Amazon Config 包含的内联策略具有其记录的配置详细信息。有关内联策略的更多信息，请参阅托管策略与内联策略(在 IAM 用户指南中)。

Amazon Key Management Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Key Management Service	AWS::KMS::Key	NA	NA

Amazon Lambda 函数

Amazon 服务	资源类型值	关系	相关资源
Amazon Lambda 函数	AWS::Lambda::Function	关联到	IAM 角色
			EC2 安全组
		包含在	EC2 子网

Amazon Network Firewall

Amazon 服务	资源类型值	关系	相关资源
Amazon Network Firewall	AWS::NetworkFirewall::Firewall	连接到	EC2 子网
		关联到	NetworkFirewall FirewallPolicy
	AWS::NetworkFirewall::FirewallPolicy	关联到	NetworkFirewall RuleGroup
	AWS::NetworkFirewall::RuleGroup	NA	NA

Amazon Secrets Manager

Amazon 服务	资源类型值	关系	相关资源
Amazon Secrets Manager	AWS::SecretsManager::Secret	关联到	Lambda 函数
		关联到	KMS 密钥

Amazon Service Catalog

Amazon 服务	资源类型值	关系	相关资源
Amazon Service Catalog	AWS::ServiceCatalog::CloudFormationProduct	包含在	产品组合
		关联到	CloudFormationProvisionedProduct
	AWS::ServiceCatalog::CloudFormationProvisionedProduct	关联到	产品组合
			CloudFormationProduct
			CloudFormationStack
	AWS::ServiceCatalog::Portfolio	包含	CloudFormationProduct

Amazon Shield

Amazon 服务	资源类型值	关系	相关资源
Amazon Shield*	AWS::Shield::Protection	关联到	亚马逊 CloudFront 分布
	AWS::ShieldRegional::Protection	关联到	EC2 EIP
		关联到	ElasticLoadBalancing Balan
		关联到	ElasticLoadBalancingV2 LoadBalancer

*对 AWS::Shield::Protection 的 Amazon Config 支持仅在美国东部（弗吉尼亚北部）区域提供。这些区域有：AWS::ShieldRegional::Protection在所有区域提供Amazon Shield支持。

Amazon Step Functions

Amazon 服务	资源类型值	关系	相关资源
Amazon Step Functions	AWS::StepFunctions::Activity	NA	NA
	AWS::StepFunctions::StateMachine	NA	NA

Amazon Systems Manager

Amazon 服务	资源类型值	关系	相关资源
Amazon Systems Manager	AWS::SSM::ManagedInstanceInventory*	关联到	EC2 实例
	AWS::SSM::PatchCompliance	关联到	托管实例清单
	AWS::SSM::AssociationCompliance	关联到	托管实例清单
	AWS::SSM::FileData	关联到	托管实例清单

*要了解有关托管实例清单的更多信息，请参阅Recording Software Configuration for Managed Instances (p. 81)。

Amazon WAF

Amazon 服务	资源类型值	关系	相关资源
Amazon WAF*	AWS::WAF::RateBasedRule	NA	NA
	AWS::WAF::Rule	NA	NA
	AWS::WAF::WebACL	关联到	WAF 规则
			WAF 基于速率的规则
			WAF 规则组
	AWS::WAF::RuleGroup	关联到	WAF 规则
	AWS::WAFRegional::RateBasedRule	NA	NA
	AWS::WAFRegional::Rule	NA	NA
	AWS::WAFRegional::WebACL	关联到	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional 规则
			WAFRegional 基于速率的规则

Amazon 服务	资源类型值	关系	相关资源
			WAFRegional ru
	AWS::WAFRegional::RuleGroup	关联到	WAFRegional 规则

*这些区域有：AmazonWAF 资源类型值仅在美国东部 (弗吉尼亚北部) 区域提供。AWS::WAFRegional::RateBasedRule、AWS::WAFRegional::Rule、AWS::WAFRegional::WebACL 和 AWS::WAFRegional::RuleGroup 在所有支持 Amazon WAF 的区域提供。

Amazon 服务	资源类型值	关系	相关资源
Amazon WAFv2*	AWS::WAFv2::WebACL	关联到	ElasticLoadBalancingV2 LoadBalancer
			ApiGateway 阶段
			WAFv2 IPSet
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup
			WAFv2 ManagedRuleSet
	AWS::WAFv2::RuleGroup	关联到	WAFv2 IPSet
			WAFv2 RegexPatternSet
	AWS::WAFv2::ManagedRuleSet	关联到	WAFv2 RuleGroup
	AWS::WAFv2::IPSet	NA	NA
	AWS::WAFv2::RegexPatternSet	NA	NA

*这些区域有：AmazonWAFv2 资源类型值在所有Amazon Web Services 区域哪里Amazon支持 WAFv2。

Amazon X-Ray

Amazon 服务	资源类型值	关系	相关资源
Amazon X-Ray	AWS::XRay::EncryptionConfig	NA	NA

Elastic Load Balancing

Amazon 服务	资源类型值	关系	相关资源
Elastic Load Balancing	Application Load Balancer AWS::ElasticLoadBalancingV2::LoadBalancer	关联到	EC2 安全组
		挂载到	子网

Amazon 服务	资源类型值	关系	相关资源
		包含在	Virtual Private Cloud (VPC)
	Application Load Balancer 侦听器 `AWS::ElasticLoadBalancingV2::Listener`	NA	NA
	Classic Load Balancer `AWS::ElasticLoadBalancing::LoadBalancer`	关联到	EC2 安全组
		挂载到	子网
		包含在	Virtual Private Cloud (VPC)
	Network Load Balancer `AWS::ElasticLoadBalancingV2::LoadBalancer`	NA	NA

配置项的组成部分

配置项由以下部分组成。

组件	说明	Contains
Metadata	有关此配置项的信息	• 版本 ID • 捕获配置项的时间 • 表明项目是否成功捕获的配置项状态 • 表明资源配置项排序的状态 ID
属性	资源属性	• 资源 ID • 此资源的键值标签列表 • 资源类型；请参阅支持的资源类型 (p. 7) • Amazon Resource Name (ARN) • 包含此资源的可用区（如果适用） • 资源创建的时间
关系	该资源和与账户关联的其他资源的关系	关系描述，例如 Amazon EBS 卷`vol-1234567`挂载到 Amazon EC2 实例`i-a1b2c3d4`
当前配置	通过对资源进行 Describe 或 List API 调用返回的信息	例如，`DescribeVolumes` API 会返回有关卷的以下信息： • 卷所在的可用区 • 卷挂载的时间 • 卷挂载到的 EC2 实例的 ID • 卷的当前状态 • 状态DeleteOn终止标志 • 卷挂载到的设备 • 卷类型，例如 `gp2`, `io1`, 或 `standard`

注意

1. 配置项关系不包含网络流或数据流依赖关系。无法自定义配置项来表示您的应用程序架构。
2. Amazon Config不记录的键值标签CloudTrail跟踪CloudFront串流分配。
3. 从 1.3 版开始，relatedEvents 字段为空。您可以访问LookupEventsAPI中的Amazon CloudTrailAPI 参考来检索资源的事件。
4. 从 1.3 版开始，configurationItemMD5Hash 字段为空。您可以使用configurationStateId字段来确保您拥有最新的配置项。

Service Limits

下表介绍了 Amazon Config 内的限制。除非另有说明，否则可根据请求提高配额。您可以请求提高配额。

有关中的其他限制的信息Amazon，请参阅Amazon服务限制.

Amazon Config 服务限制

描述	限制值	能否增加
最大 Amazon Config 规则数（每个区域、每个账户）	400	是
最大配置聚合器数	50	是
聚合器中的最大帐户数	10000	否
所有聚合器每周添加或删除的最大账户数量	1000	是
最大标签数	50	否
单个账户和区域中保存的查询的最大数量	300	是

单个账户一致性包

描述	限制值	能否增加
每个账户的最大一致性包数	50	否
每个一致性包最多 Amazon Config 条规则	130	否
所有一致性包中每个账户最多 Amazon Config 条规则	150	否

组织一致性包

描述	限制值	能否增加
每个组织的最大一致性包数	50	否
每个组织一致性包最多 Amazon Config 条规则	130	否

描述	限制值	能否增加
所有组织一致性包中每个账户最多 Amazon Config 条规则	180	否

组织配置规则

描述	限制值	能否增加
每个组织的最大组织 Amazon Config 规则数	150	否

开始使用 Amazon Config

注册 Amazon 后，您的账户将获得所有 Amazon 服务的访问权限。您只需为使用的服务付费。

如果您还没有 Amazon Web Services 账户，请完成以下步骤来创建一个。

注册 Amazon Web Services 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，您将接到一通电话，要求您使用电话键盘输入一个验证码。

在您注册 Amazon 账户之后，您可以通过 Amazon Web Services Management Console、Amazon CLI 或 Amazon 开发工具包开始使用 Amazon Config。使用控制台可以加快和简化流程。

在您设置 Amazon Config 时，可以完成以下操作：

- 指定您希望 Amazon Config 记录的资源类型。
- 设置 Amazon S3 存储桶以接收配置快照（在需要时）和配置历史记录。
- 设置 Amazon SNS 主题以发送配置流通知。
- GrantAmazon Config用于访问 Amazon S3 存储桶和 SNS 主题的权限。
- 指定您希望 Amazon Config 评估所记录资源类型的合规性信息使用的规则。

有关如何使用 Amazon CLI的更多信息，请参阅使用 Amazon CLI 设置 Amazon Config (p. 29)。

有关如何使用 Amazon SDKs 的更多信息，请参阅适用于 Amazon Config 的 Amazon 软件开发工具包 (p. 281)。

主题

使用控制台设置 Amazon Config

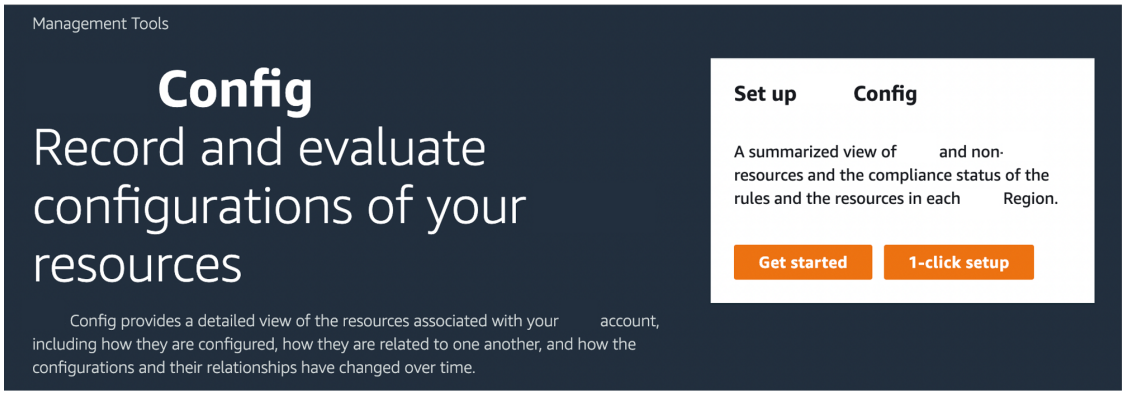
您可以使用 Amazon Web Services Management Console来开始使用 Amazon Config 执行以下操作：

- 指定您希望 Amazon Config 记录的资源类型。
- 设置 Amazon SNS 以通知您配置更改。
- 指定 Amazon S3 存储桶。
- AddAmazon Config托管规则以评估资源类型。

如果您是首次使用 Amazon Config 或者为新区域配置 Amazon Config，则可以选择托管规则来评估资源配置。对于支持的区域Amazon Config和Amazon Config规则，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.

使用控制台设置 Amazon Config

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 如果这是您首次打开 Amazon Config 控制台或在新区域中设置 Amazon Config，Amazon Config 控制台页面的外观与以下类似：



3. 选择一键设置启动Amazon Config基于Amazon最佳实践。还可以选择试用，请您自己完成以下步骤。
4. 在 Settings (设置) 页面上，对于 Resource types to record (要记录的资源类型)，指定您希望 Amazon Config 记录的所有资源类型。这些资源类型是 Amazon 资源或第三方资源或自定义资源。

   - 记录该区域支持的所有资源
     - Amazon Config记录受支持的配置更改Amazon资源类型以及在中注册的第三方资源类型Amazon CloudFormation注册机构。Amazon Config自动开始录制新支持Amazon资源类型。Amazon Config还会自动开始记录第三方资源，自定义资源类型是通过Amazon CloudFormation.
     - 选择包含全球资源以记录支持的全局资源类型（如 IAM 资源）。Amazon Config会自动开始记录新的支持的全局资源类型。
   - 记录特定资源类型
     - Amazon Config仅记录您指定的资源类型的配置更改。

   有关这些选项的详细信息，请参阅 选择 Amazon Config 所记录的资源 (p. 73)。
5. 适用于Amazon Config角色，选择现有的Amazon Config服务相关角色，或通过输入您的账户 ID 从您的账户中选择一个角色。服务相关角色由预先定义Amazon Config，并包含该服务调用 otherAmazon服务。
6. 适用于传送方式，选择 Amazon S3 存储桶Amazon Config发送配置历史记录文件和配置快照文件

   - 创建存储桶— 对于S3 存储桶名称，键入 Amazon S3 存储桶的名称。

     您键入的名称在 Amazon S3 中的所有现有存储桶名称中必须唯一。添加前缀（例如，您所在组织的名称）是确保唯一性的一种方法。存储桶创建完毕后，您无法更改其名称。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的存储桶限制。
   - Choose (从您的账户选择一个存储桶)— 对于S3 存储桶名称，选择您的首选存储桶。
   - 从另一个账户中选择一个存储桶— 对于S3 存储桶名称，请键入存储桶名称。

     Note

     如果您从其他账户选择存储桶，则该存储桶必须拥有授予 Amazon Config 访问权限的策略。有关更多信息，请参阅 Amazon S3 存储桶的权限 (p. 221)。

7. 适用于Amazon SNS 主题，选择将配置配置更改流式传输到 Amazon SNS 主题有Amazon Config发送通知，例如配置历史记录传递、配置快照传送和合规性。
8. 在选择有Amazon Config将信息流式传输到 Amazon SNS 主题，请选择目标主题：
   - 创建主题— 对于主题名称，键入您的 SNS 主题的名称。
   - 从你的账户中选择一个主题— 对于主题名称，选择您的首选主题。
   - 从另一个账户中选择一个主题— 对于主题 ARN，请键入主题的 Amazon 资源名称 (ARN)。如果您从其他账户选择主题，则该主题必须拥有授予 Amazon Config 访问权限的策略。有关更多信息，请参阅 Amazon SNS 主题的权限 (p. 225)。

     Note

     Amazon SNS 主题所在的区域必须与您设置的区域相同Amazon Config.
9. 如果您在支持规则的区域中设置 Amazon Config，请选择 Next (下一步)。请参阅 使用Amazon Config控制台规则 (p. 52)。

   否则，请选择确认.

有关查找账户中现有资源及了解资源配置的信息，请参阅 查看 Amazon 资源配置和历史记录 (p. 57)。

您还可使用Amazon Simple Queue ServicAmazon以编程方式资源：有关更多信息，请参阅 监控 AmazonAmazon SQS 的资源变更 (p. 274)。

使用 Amazon CLI 设置 Amazon Config

您可以使用 Amazon Command Line Interface 控制和自动执行 Amazon 服务。

有关的更多信息Amazon CLI以及有关安装Amazon CLItoose，请参阅以下的Amazon Command Line Interface用户指南.

- Amazon Command Line Interface 用户指南
- 开始设置 Amazon Command Line Interface

请参阅以下主题以使用 Amazon CLI 设置 Amazon Config。当您设置 Amazon Config 之后，您可以添加规则来评估您账户中的资源类型。有关使用 Amazon Config 设置规则的更多信息，请参阅查看、更新和删除规则 (Amazon CLI) (p. 206)。

主题

先决条件

在设置之前Amazon用Amazon CLI，您需要创建一个 Amazon S3 存储桶、一个 Amazon SNS 主题和一个 IAM 角色，并将附加的策略作为先决条件。然后，您可以使用 Amazon CLI 为 Amazon Config 指定存储桶、主题和角色。按照此过程设置您的先决条件Amazon Config.

目录

- 创建 IAM 角色 (p. 42)

创建 Amazon S3 存储桶

如果您的账户中已经存在 Amazon S3 存储桶并且您想要使用该存储桶，请跳过本步骤并转至创建 Amazon SNS 主题 (p. 34).

使用 S3 控制台

创建存储桶

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 选择 Create bucket (创建存储桶)。
3. 在 Bucket name (存储桶名称) 中，输入符合 DNS 标准的存储桶名称。

   存储桶名称必须满足以下要求：

   - 在所有 Amazon S3 中是唯一的。
   - 长度必须介于 3 到 63 个字符之间。
   - 不包含大写字符。
   - 以小写字母或数字开头。

   创建存储桶后，便无法再更改其名称。请确保所选的存储桶名称在 Amazon S3 中的所有现有存储桶名称中是唯一名称。有关存储桶命名规则和约定的更多信息，请参阅存储桶限制中的Amazon Simple Storage S.

   > Important
   >
   > 避免在存储桶名称中包含敏感信息，如账号。存储桶名称会显示在指向存储桶中的对象的 URL 中。

4. 对于 Region（区域），选择要放置存储桶的Amazon区域。

   请选择一个靠近您的区域可最大程度地减少延迟和成本以及满足法规要求。在某一地区存储的对象将一直留在该地区，除非您特意将其转移到其他地区。有关 Amazon S3 Amazon区域的列表，请参阅亚马逊云科技一般参考中的Amazon服务终端节点。

5. 在 Bucket settings for Block Public Access (阻止公有访问的存储桶设置) 中，请选择要应用于存储桶的 Block Public Access (阻止公有访问) 设置。

   我们建议您将所有设置保持为启用状态，除非您知道您需要为您的使用案例关闭其中一个或多个设置，例如托管公共网站。您为存储桶启用的阻止公有访问设置也将为您在存储桶上创建的所有访问点启用。有关阻止公有访问的更多信息，请参阅使用 Amazon S3 阻止公有访问中的Amazon Simple Storage S.

6. （可选）如果要启用 S3 对象锁定：

   a. 请选择 Advanced settings (高级设置)，然后阅读显示的消息。

      > Important
      >
      > 您只能在创建存储桶时为其启用 S3 对象锁定。如果您为存储桶启用了对象锁定，则以后无法禁用它。启用对象锁定还会启用存储桶的版本控制。为存储桶启用对象锁定后，必须先配置对象锁定设置，然后才能保护存储桶中的任何对象。有关配置对象保护的更多信息，请参阅使用 Amazon S3 控制台配置 S3 对象锁定.

   b. 如果要启用对象锁定，请在文本框中输入 enable 并选择 Confirm (确认)。

   有关 S3 对象锁的更多信息，请参阅使用 Amazon S3 对象锁定以锁定对象中的Amazon Simple Storage S.

7. 请选择 Create bucket (创建存储桶)。

使用 Amazon 软件开发工具包

使用 Amazon 软件开发工具包创建存储桶时，您必须先创建一个客户端，然后使用该客户端发送创建存储桶的请求。作为最佳做法，您应在同一 Amazon Web Services 区域 中创建客户端和存储桶。如果您在创建客户端或存储桶时未指定区域，Amazon S3 将使用默认区域美国东部（弗吉尼亚北部）。

要创建客户端来访问双堆栈终端节点，则必须指定 Amazon Web Services 区域。有关更多信息，请参阅 。Amazon S3 双堆栈终端节点. 有关可用 Amazon Web Services 区域 的列表，请参阅《Amazon 一般参考》中的区域和终端节点。

创建客户端时，区域映射到特定于区域的终端节点。客户端使用此终端节点与 Amazon S3 进行通信：`s3.<region>.amazonaws.com`. 如果您的区域是在 2019 年 3 月 20 日之后启动的，则您的客户端和存储桶必须位于同一区域。不过，您可以使用美国东部（弗吉尼亚北部）区域中的客户端在 2019 年 3 月 20 日之前启动的任何区域中创建存储桶。有关更多信息，请参阅 。传统终端节点.

这些 Amazon 软件开发工具包代码示例执行以下任务：

- 通过明确指定 Amazon Web Services 区域 创建客户端 – 在本示例中，客户端使用 `s3.us-west-2.amazonaws.com` 终端节点与 Amazon S3 通信。您可以指定任意 Amazon Web Services 区域。有关 Amazon Web Services 区域 的列表，请参阅《Amazon 一般参考》中的区域和终端节点。
- 通过仅指定存储桶名称来发送创建存储桶请求 — 客户端向 Amazon S3 发送请求，请求在您创建客户端的区域中创建存储桶。
- 检索有关存储桶位置的信息 — Amazon S3 将存储桶位置信息存储在与存储桶关联的位置子资源中。

Java

此示例说明如何使用 Amazon SDK for Java 创建 Amazon S3 存储桶。有关创建和测试有效示例的说明，请参阅测试 Amazon S3 Java 代码示例.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.GetBucketLocationRequest;

import java.io.IOException;

public class CreateBucket2 {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            if (!s3Client.doesBucketExistV2(bucketName)) {
                // Because the CreateBucketRequest object doesn't specify a region, the
                // bucket is created in the region specified in the client.
                s3Client.createBucket(new CreateBucketRequest(bucketName));
```

```
                // Verify that the bucket was created by retrieving it and checking its
 location.
                String bucketLocation = s3Client.getBucketLocation(new
 GetBucketLocationRequest(bucketName));
                System.out.println("Bucket location: " + bucketLocation);
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

有关如何创建和测试有效示例的信息，请参阅运行 Amazon S3 .NET 代码示例.

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using Amazon.S3.Util;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CreateBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion = RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CreateBucketAsync().Wait();
        }

        static async Task CreateBucketAsync()
        {
            try
            {
                if (!(await AmazonS3Util.DoesS3BucketExistAsync(s3Client, bucketName)))
                {
                    var putBucketRequest = new PutBucketRequest
                    {
                        BucketName = bucketName,
                        UseClientRegion = true
                    };

                    PutBucketResponse putBucketResponse = await
 s3Client.PutBucketAsync(putBucketRequest);
                }
                // Retrieve the bucket location.
                string bucketLocation = await FindBucketLocationAsync(s3Client);
            }
```

```
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
        static async Task<string> FindBucketLocationAsync(IAmazonS3 client)
        {
            string bucketLocation;
            var request = new GetBucketLocationRequest()
            {
                BucketName = bucketName
            };
            GetBucketLocationResponse response = await
 client.GetBucketLocationAsync(request);
            bucketLocation = response.Location.ToString();
            return bucketLocation;
        }
    }
}
```

Ruby

有关如何创建和测试有效示例的信息，请参阅使用Amazon适用于 SDK for Ruby（版本 3）.

Example

```
require "aws-sdk-s3"

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name. This
 is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      "None. You must create a bucket before you can get it's location!"
    else
      @bucket.client.get_bucket_location(bucket: @bucket.name).location_constraint
```

```
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("doc-example-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

使用 Amazon CLI

您也可以使用Amazon Command Line Interface (Amazon CLI) 创建 S3 存储桶。有关更多信息，请参阅《Amazon CLI 命令参考》中的 create-bucket。

有关 Amazon CLI 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的什么是 Amazon Command Line Interface？。

> Note
>
> 您也可以使用另一账户的 Amazon S3 存储桶，不过您可能需要为该存储桶创建策略以便向授予访问权限Amazon Config. 有关向 Amazon S3 存储桶授予权限的信息，请参阅Amazon S3 存储桶的权限 (p. 221)，然后转到创建 Amazon SNS 主题 (p. 34).

创建 Amazon SNS 主题

如果您的账户中已经存在 Amazon SNS 主题并且您想要使用该主题，请跳过本步骤并转至创建 IAM 角色 (p. 42).

使用 SNS 控制台

创建 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：https://console.aws.amazon.com/sns/v3/home。
2. 请执行下列操作之一：
   - 如果之前未在您的 Amazon Web Services 账户 下创建主题，请阅读主页上的 Amazon SNS 的描述。
   - 如果之前已在您的 Amazon Web Services 账户 下创建主题，请在导航面板上选择 Topics（主题）。
3. 在 Topics（主页）页面上，选择 Create topic（创建主题）。
4. 在 Create topic（创建主题）页面上，在 Details（详细信息）部分中，执行以下操作：
   a. 对于 Type（类型），选择主题类型（标准或者FIFO）。
   b. 输入主题的名称。对于 FIFO 主题，将 .fifo 添加到名称的末尾。
   c. （可选）输入主题的显示名称。
   d. （可选）对于 FIFO 主题，您可以选择基于内容的消息重复数据删除以启用默认的消息重复数据删除。有关更多信息，请参阅 。FIFO 主题的消息重复数据删除.
5. （可选）展开加密部分并执行以下操作。有关更多信息，请参阅静态加密。
   a. 选择 Enable encryption (启用加密)。

b. 指定客户主密钥 (CMK)。有关更多信息，请参阅 。关键术语.

对于每个 CMK 类型，都会显示 Description (描述)、Account (账户) 和 CMK ARN。

Important

如果您不是 CMK 的拥有者，或者您登录的账户没有 `kms:ListAliases` 和 `kms:DescribeKey` 权限，则无法在 Amazon SNS 控制台上查看有关 CMK 的信息。要求 CMK 拥有者授予您这些权限。有关更多信息，请参阅 。Amazon KMSAPI 权限：操作和资源参考中的Amazon Key Management Service开发人员指南.

- 默认情况下，Amazon SNS 的 Amazon 托管 CMK（默认）alias/aws/sns 被选择。

  Note

  记住以下内容：

  - 第一次使用 Amazon Web Services Management Console 为主题指定 Amazon SNS 的 Amazon 托管 CMK 时，Amazon KMS 创建 Amazon SNS 的 Amazon 托管 CMK。
  - 或者，您第一次对启用了 SSE 的主题使用 `Publish` 操作时，Amazon KMS 创建 Amazon SNS 的 Amazon 托管 CMK。
- 要从您的 Amazon 账户中使用已定义 CMK，请选择 Customer master key (CMK)（客户主密钥 (CMK)）字段，然后从列表中选择自定义 CMK。

  Note

  有关创建自定义 CMK 的说明，请参阅 Amazon Key Management Service 开发人员指南中的创建密钥
- 要从您的 Amazon 账户或另一个 Amazon 账户中使用使用自定义 CMK ARN，请将其输入到 Customer master key (CMK)（客户主密钥 (CMK)）字段中。

6. （可选）默认情况下，只有主题拥有者才能发布或订阅主题。要配置其他访问权限，请展开访问策略部分。有关更多信息，请参阅 。Amazon SNS 中的 Identity and Access Management和用于 Amazon SNS 访问控制的示例案例.

   Note

   使用控制台创建主题时，默认策略使用 `aws:SourceOwner` 条件键。此密钥类似于 `aws:SourceAccount`。
7. （可选）要配置 Amazon SNS 重试失败消息传输尝试的方式，请展开 Delivery retry policy (HTTP/S)（传输重试策略 (HTTP/S)）部分。有关更多信息，请参阅 。Amazon SNS 消息传输重试.
8. （可选）配置 Amazon SNS 记录针对的消息传输的方式 CloudWatch，展开传送状态日志记录部分。有关更多信息，请参阅 。Amazon SNS 消息传输状态.
9. （可选）要将元数据标签添加到主题中，请展开标签部分，输入一个键和值（可选），然后选择添加标签。有关更多信息，请参阅 。Amazon SNS 主题标记.
10. 选择 Create topic（创建主题）。

    主题已创建，***MyTopic***屏幕上随即显示页面。

    主题的名称、ARN、（可选）显示名称和主题所有者的 Amazon 账户 ID 将显示在 Details（详细信息）部分中。
11. 将主题 ARN 复制到剪贴板，例如：

```
arn:aws:sns:us-east-2:123456789012:MyTopic
```

要使用电子邮件地址订阅 Amazon SNS 主题

1. 通过以下网址打开 Amazon SNS 控制台：https://console.aws.amazon.com/sns/v3/home。

2. 在左侧导航窗格中，选择订阅。
3. 在 Subscriptions（订阅）页面上，选择 Create subscription（创建订阅）。
4. 在 Create subscription（创建订阅）页上的 Details（详细信息）部分中，执行以下操作：

   a. 对于 Topic ARN（主题 ARN），选择主题的 Amazon Resource Name (ARN)。
   b. 对于 Protocol（协议），选择终端节点类型。可用的终端节点类型包括：

      - HTP/HTP
      - 电子邮件/电子邮件-JSON
      - Amazon Kinesis Data Firehose
      - Amazon SQS

        Note

        要订阅到 SNS FIFO 主题，请选择该选项。

      - Amazon Lambda
      - 平台应用程序终端节点
      - SMS

   c. 对于 Endpoint（终端节点），输入终端节点值，例如电子邮件地址或 Amazon SQS 队列的 ARN。
   d. 仅限于 Kinesis Data Firehose 终端节点：适用于订阅角色 ARN，指定您为写入到 Kinesis Data Firehose 传输流创建的 IAM 角色的 ARN。有关更多信息，请参阅 。订阅 Kinesis Data Firehose 传输流到 Amazon SNS 主题的先决条件.
   e. （可选）对于 Kinesis Data Firehose、Amazon SQS、HTTP/S 终端节点，您还可以启用原始消息传输。有关更多信息，请参阅 。Amazon SNS 原始消息传输.
   f. （可选）要配置筛选策略，请展开 Subscription filter policy（订阅筛选策略）部分。有关更多信息，请参阅 。Amazon SNS 订阅筛选策略.
   g. （可选）要为订阅配置死信队列，请展开 Redrive policy (dead-letter queue)（重新驱动策略（死信队列））部分。有关更多信息，请参阅 。Amazon SNS 死信队列 (DLQ).
   h. 选择 Create subscription（创建订阅）。

      控制台将创建订阅并打开订阅的 Details（详细信息）页面。

使用 Amazon 软件开发工具包

要使用 Amazon 开发工具包，您必须使用您的凭证对其进行配置。有关更多信息，请参阅 Amazon 开发工具包和工具参考指南中的共享配置和凭证文件。

以下代码示例显示如何创建 Amazon SNS 主题。

.NET

Amazon SDK for .NET

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
using System;
using System.Threading.Tasks;
using Amazon.SimpleNotificationService;
using Amazon.SimpleNotificationService.Model;

/// <summary>
/// This example shows how to use Amazon Simple Notification Service
/// (Amazon SNS) to add a new Amazon SNS topic. The example was created
```

```
   /// using the AWS SDK for .NET version 3.7 and .NET Core 5.0.
   /// </summary>
   public class CreateSNSTopic
   {
       public static async Task Main()
       {
           string topicName = "ExampleSNSTopic";

           IAmazonSimpleNotificationService client = new
AmazonSimpleNotificationServiceClient();

           var topicArn = await CreateSNSTopicAsync(client, topicName);
           Console.WriteLine($"New topic ARN: {topicArn}");
       }

       /// <summary>
       /// Creates a new SNS topic using the supplied topic name.
       /// </summary>
       /// <param name="client">The initialized SNS client object used to
       /// create the new topic.</param>
       /// <param name="topicName">A string representing the topic name.</param>
       /// <returns>The Amazon Resource Name (ARN) of the created topic.</returns>
       public static async Task<string>
CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
       {
           var request = new CreateTopicRequest
           {
               Name = topicName,
           };

           var response = await client.CreateTopicAsync(request);

           return response.TopicArn;
       }

   }
```

- 有关详细信息，请参阅。CreateTopic在Amazon SDK for .NETAPI 参考.

C++

适用于 C++ 的 SDK

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
Aws::SDKOptions options;
Aws::InitAPI(options);
{
  Aws::String topic_name = argv[1];
  Aws::SNS::SNSClient sns;

  Aws::SNS::Model::CreateTopicRequest ct_req;
  ct_req.SetName(topic_name);

  auto ct_out = sns.CreateTopic(ct_req);

  if (ct_out.IsSuccess())
  {
    std::cout << "Successfully created topic " << topic_name << std::endl;
```

```
    }
    else
    {
      std::cout << "Error creating topic " << topic_name << ":" <<
        ct_out.GetError().GetMessage() << std::endl;
    }
  }

  Aws::ShutdownAPI(options);
```

- 有关详细信息，请参阅。CreateTopic在Amazon SDK for C++API 参考.

Go

SDK for Go V2

Tip

要了解如何设置和运行此示例，请参阅GitHub.

- 有关详细信息，请参阅。CreateTopic在Amazon SDK for GoAPI 参考.

Java

SDK for Java 2.x

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
public static String createSNSTopic(SnsClient snsClient, String topicName ) {

    CreateTopicResponse result = null;
    try {
        CreateTopicRequest request = CreateTopicRequest.builder()
                .name(topicName)
                .build();

        result = snsClient.createTopic(request);
        return result.topicArn();
    } catch (SnsException e) {

        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
    return "";
}
```

- 有关详细信息，请参阅。CreateTopic在Amazon SDK for Java 2.xAPI 参考.

JavaScript

适用于的开发工具包 JavaScript V3

Tip

要了解如何设置和运行此示例，请参阅GitHub.

在单独的模块中创建客户端并将其导出。

```
import  { SNSClient } from "@aws-sdk/client-sns";
// Set the AWS Region.
const REGION = "REGION"; //e.g. "us-east-1"
// Create SNS service object.
const snsClient = new SNSClient({ region: REGION });
export  { snsClient };
```

导入软件开发工具包和客户端模块，然后调用 API。

```
// Import required AWS SDK clients and commands for Node.js
import {CreateTopicCommand } from "@aws-sdk/client-sns";
import {snsClient } from "./libs/snsClient.js";

// Set the parameters
const params = { Name: "TOPIC_NAME" }; //TOPIC_NAME

const run = async () => {
  try {
    const data = await snsClient.send(new CreateTopicCommand(params));
    console.log("Success.",  data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err.stack);
  }
};
run();
```

- 有关更多信息，请参阅 Amazon SDK for JavaScript 开发人员指南。
- 有关详细信息，请参阅。CreateTopic在Amazon SDK for JavaScriptAPI 参考.

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
suspend fun createSNSTopic(topicName: String): String {

       val request = CreateTopicRequest {
            name = topicName
        }

       SnsClient { region = "us-east-1" }.use { snsClient ->
        val result = snsClient.createTopic(request)
        return result.topicArn.toString()
       }
 }
```

- 有关详细信息，请参阅。CreateTopic在AmazonSDK for Kotlin API 参考.

PHP

SDK for PHP

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
require 'vendor/autoload.php';

use Aws\Sns\SnsClient;
use Aws\Exception\AwsException;

/**
 * Create a Simple Notification Service topics in your AWS account at the requested
 region.
 *
 * This code expects that you have AWS credentials set up per:
 * https://docs.aws.amazon.com/sdk-for-php/v3/developer-guide/
guide_credentials.html
 */

$SnSclient = new SnsClient([
    'profile' => 'default',
    'region' => 'us-east-1',
    'version' => '2010-03-31'
]);

$topicname = 'myTopic';

try {
    $result = $SnSclient->createTopic([
        'Name' => $topicname,
    ]);
    var_dump($result);
} catch (AwsException $e) {
    // output error message if fails
    error_log($e->getMessage());
}
```

- 有关更多信息，请参阅 Amazon SDK for PHP 开发人员指南。
- 有关详细信息，请参阅。CreateTopic在Amazon SDK for PHPAPI 参考.

Python

适用于 Python (Boto3) 的 SDK

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""
    def __init__(self, sns_resource):
        """
```

```
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource

    def create_topic(self, name):
        """
        Creates a notification topic.

        :param name: The name of the topic to create.
        :return: The newly created topic.
        """
        try:
            topic = self.sns_resource.create_topic(Name=name)
            logger.info("Created topic %s with ARN %s.", name, topic.arn)
        except ClientError:
            logger.exception("Couldn't create topic %s.", name)
            raise
        else:
            return topic
```

- 有关详细信息，请参阅。CreateTopic在AmazonSDK for Python (Boto3) 的 SDK API 参考.

Ruby

SDK for Ruby

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
require 'aws-sdk-sns'  # v2: require 'aws-sdk'

def topic_created?(sns_client, topic_name)

sns_client.create_topic(name: topic_name)
rescue StandardError => e
  puts "Error while creating the topic named '#{topic_name}': #{e.message}"
end

# Full example call:
def run_me
  topic_name = 'TOPIC_NAME'
  region = 'REGION'

  sns_client = Aws::SNS::Client.new(region: region)

  puts "Creating the topic '#{topic_name}'..."

  if topic_created?(sns_client, topic_name)
    puts 'The topic was created.'
  else
    puts 'The topic was not created. Stopping program.'
    exit 1
  end
end

run_me if $PROGRAM_NAME == __FILE__
```

- 有关更多信息，请参阅 Amazon SDK for Ruby 开发人员指南。

- 有关详细信息，请参阅。CreateTopic在Amazon SDK for RubyAPI 参考.

Rust

SDK for Rust

Note

本文档适用于预览版中的软件开发工具包。软件开发工具包可能随时发生变化，不应在生产环境中使用。

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
async fn make_topic(client: &Client, topic_name: &str) -> Result<(), Error> {
    let resp = client.create_topic().name(topic_name).send().await?;

    println!(
        "Created topic with ARN: {}",
        resp.topic_arn().unwrap_or_default()
    );

    Ok(())
}
```

- 有关详细信息，请参阅。CreateTopic在AmazonSDK for Rust API 参考.

使用 Amazon CLI

您也可以使用Amazon Command Line Interface(Amazon CLI) 以创建 Amazon SNS 主题。有关更多信息，请参阅 。创建主题中的Amazon CLI命令参考.

有关 Amazon CLI 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的什么是 Amazon Command Line Interface？。

Note

您也可以使用另一账户的 Amazon SNS 主题，但在这种情况下，您可能需要为该主题创建策略，以便向授予访问权限Amazon Config. 有关向 Amazon SNS 主题授予权限的信息，请参阅Amazon SNS 主题的权限 (p. 225)然后转到创建 IAM 角色 (p. 42).

创建 IAM 角色

使用 IAM 控制台

您可使用 IAM 控制台创建 IAM 角色Amazon Config访问您的 Amazon S3 存储桶、访问 Amazon SNS 主题以及获取受支持的配置详细信息Amazon资源的费用。当您使用控制台创建 IAM 角色时，Amazon Config会自动为您附加该角色所需的权限。

为创建角色Amazon服务

1. 登录 Amazon Web Services Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择 Roles，然后选择 Create role。

3. 适用于选择可信任的实体，选择Amazon服务.
4. 选择您想要的使用案例Amazon Config：Config — 可自定义、Config — Organizations、Config，或者Config：一致性包. 然后选择下一步。
5. 在存储库的命名、审核和创建页面，查看您的角色的详细信息，然后选择创建角色.

使用 Amazon 软件开发工具包

要使用 Amazon 开发工具包，您必须使用您的凭证对其进行配置。有关更多信息，请参阅 Amazon 开发工具包和工具参考指南中的共享配置和凭证文件。

以下代码示例显示如何创建 IAM 角色。

.NET

Amazon SDK for .NET

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
        /// <summary>
        /// Create a new IAM role which we can attach to a user.
        /// </summary>
        /// <param name="client">The initialized IAM client object.</param>
        /// <param name="roleName">The name of the IAM role to create.</param>
        /// <param name="rolePermissions">The permissions which the role will
have.</param>
        /// <returns>A Role object representing the newly created role.</returns>
        public static async Task<Role> CreateRoleAsync(
            AmazonIdentityManagementServiceClient client,
            string roleName,
            string rolePermissions)
        {
            var request = new CreateRoleRequest
            {
                RoleName = roleName,
                AssumeRolePolicyDocument = rolePermissions,
            };

            var response = await client.CreateRoleAsync(request);

            return response.Role;
        }
```

- 有关详细信息，请参阅。CreateRole在Amazon SDK for .NETAPI 参考.

Go

SDK for Go V2

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
// CreateRole
```

```
myRole, err := service.CreateRole(context.Background(), &iam.CreateRoleInput{
 RoleName:    aws.String(ExampleRoleName),
 Description: aws.String("My super awesome example role"),
 AssumeRolePolicyDocument: aws.String(`{
  "Version": "2012-10-17",
  "Statement": [
    {
   "Effect": "Allow",
   "Principal": {
     "Service": "ec2.amazonaws.com"
   },
   "Action": "sts:AssumeRole"
    }
  ]
   }`),
})

if err != nil {
 panic("Couldn't create role: " + err.Error())
}

fmt.Println("## Create Role")
fmt.Printf("The new role's ARN is %s \n", *myRole.Role.Arn)
```

- 有关详细信息，请参阅。CreateRole在Amazon SDK for GoAPI 参考.

Java

SDK for Java 2.x

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
   public static String createIAMRole(IamClient iam, String rolename, String
fileLocation ) throws Exception {

       try {
           JSONObject jsonObject = (JSONObject) readJsonSimpleDemo(fileLocation);
           CreateRoleRequest request = CreateRoleRequest.builder()
                   .roleName(rolename)
                   .assumeRolePolicyDocument(jsonObject.toJSONString())
                   .description("Created using the AWS SDK for Java")
                   .build();

           CreateRoleResponse response = iam.createRole(request);
           System.out.println("The ARN of the role is "+response.role().arn());

       } catch (IamException e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
       }
       return "";
   }

   public static Object readJsonSimpleDemo(String filename) throws Exception {
       FileReader reader = new FileReader(filename);
       JSONParser jsonParser = new JSONParser();
       return jsonParser.parse(reader);
   }
```

```
```

- 有关详细信息，请参阅。CreateRole在Amazon SDK for Java 2.xAPI 参考.

JavaScript

适用于的开发工具包 JavaScript V3

Tip

要了解如何设置和运行此示例，请参阅GitHub.

创建客户端。

```
import { IAMClient } from "@aws-sdk/client-iam";
// Set the AWS Region.
const REGION = "REGION"; // For example, "us-east-1".
// Create an IAM service client object.
const iamClient = new IAMClient({ region: REGION });
export { iamClient };
```

创建角色。

```
// Import required AWS SDK clients and commands for Node.js.
import { iamClient } from "./libs/iamClient.js";
import { CreateRoleCommand } from "@aws-sdk/client-iam";

// Sample assume role policy JSON.
const role_json = {
    Version: "2012-10-17",
    Statement: [
        {
            Effect: "Allow",
            Principal: {
                AWS: "USER_ARN", // The ARN of the user.
            },
            Action: "sts:AssumeRole",
        },
    ],
};
// Stringify the assume role policy JSON.
const myJson = JSON.stringify(role_json);

// Set the parameters.
const params = {
    AssumeRolePolicyDocument: myJson,
    Path: "/",
    RoleName: "ROLE_NAME"
};

const run = async () => {
    try {
        const data = await iamClient.send(new CreateRoleCommand(params));
        console.log("Success. Role created. Role Arn: ", data.Role.RoleName);
        } catch (err) {
            console.log("Error", err);
        }
};
run();
```

- 有关详细信息，请参阅。CreateRole在Amazon SDK for JavaScriptAPI 参考.

PHP

SDK for PHP

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
$uuid = uniqid();
$service = new IamService();

$assumeRolePolicyDocument = "{
                \"Version\": \"2012-10-17\",
                \"Statement\": [{
                    \"Effect\": \"Allow\",
                    \"Principal\": {\"AWS\": \"{$user['Arn']}\"},
                    \"Action\": \"sts:AssumeRole\"
                }]
            }";
$assumeRoleRole = $service->createRole("iam_demo_role_$uuid",
 $assumeRolePolicyDocument);
echo "Created role: {$assumeRoleRole['RoleName']}\n";

    /**
     * @param string $roleName
     * @param string $rolePolicyDocument
     * @return array
     * @throws AwsException
     */
    public function createRole(string $roleName, string $rolePolicyDocument)
    {
        $result = $this->customWaiter(function () use ($roleName,
 $rolePolicyDocument) {
            return $this->iamClient->createRole([
                'AssumeRolePolicyDocument' => $rolePolicyDocument,
                'RoleName' => $roleName,
            ]);
        });
        return $result['Role'];
    }
```

- 有关详细信息，请参阅。CreateRole在Amazon SDK for PHPAPI 参考.

Python

适用于 Python (Boto3) 的 SDK

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
def create_role(role_name, allowed_services):
    """
    Creates a role that lets a list of specified services assume the role.
```

```
    :param role_name: The name of the role.
    :param allowed_services: The services that can assume the role.
    :return: The newly created role.
    """
    trust_policy = {
        'Version': '2012-10-17',
        'Statement': [{
                'Effect': 'Allow',
                'Principal': {'Service': service},
                'Action': 'sts:AssumeRole'
            } for service in allowed_services
        ]
    }

    try:
        role = iam.create_role(
            RoleName=role_name,
            AssumeRolePolicyDocument=json.dumps(trust_policy))
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

- 有关详细信息，请参阅。CreateRole在AmazonSDK for Python (Boto3) 的 SDK API 参考.

Ruby

SDK for Ruby

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
 # Creates a role that can be assumed by a user.
 #
 # @param role_name [String] The name to give the role.
 # @param user [Aws::IAM::User] The user who is granted permission to assume the
role.
 # @return [Aws::IAM::Role] The newly created role.
 def create_role(role_name, user)
   role = @iam_resource.create_role(
     role_name: role_name,
     assume_role_policy_document: {
       Version: "2012-10-17",
       Statement: [{
         Effect: "Allow",
         Principal: {'AWS': user.arn},
         Action: "sts:AssumeRole"
       }]
     }.to_json)
   puts("Created role #{role.name}.")
 rescue Aws::Errors::ServiceError => e
   puts("Couldn't create a role for the demo. Here's why: ")
   puts("\t#{e.code}: #{e.message}")
   raise
 else
   role
 end
```

- 有关详细信息，请参阅。CreateRole在Amazon SDK for RubyAPI 参考.

Rust

SDK for Rust

Note

本文档适用于预览版中的软件开发工具包。软件开发工具包可能随时发生变化，不应在生产环境中使用。

Tip

要了解如何设置和运行此示例，请参阅GitHub.

```
pub async fn create_role(
    client: &iamClient,
    role_name: &str,
    role_policy_document: &str,
) -> Result<Role, iamError> {
    let response: CreateRoleOutput = loop {
        if let Ok(response) = client
            .create_role()
            .role_name(role_name)
            .assume_role_policy_document(role_policy_document)
            .send()
            .await
        {
            break response;
        }
    };

    Ok(response.role.unwrap())
}
```

- 有关详细信息，请参阅。CreateRole在AmazonSDK for Rust API 参考.

使用 Amazon CLI

您也可以使用Amazon Command Line Interface(Amazon CLI) 以创建 Amazon SNS 主题。有关更多信息，请参阅 。create-role中的Amazon CLI命令参考. 然后，您可以使用将策略附加到角色attach-role-policy命令。

有关 Amazon CLI 的更多信息，请参阅《Amazon Command Line Interface 用户指南》中的什么是 Amazon Command Line Interface？。

启用 Amazon Config

Note

在设置之前Amazon Config用Amazon CLI，您需要创建一个 Amazon S3 存储桶、一个 Amazon SNS 主题和一个 IAM 角色，并将附加的策略作为先决条件。然后，您可以使用 Amazon CLI 为 Amazon Config 指定存储桶、主题和角色。设置您的先决条件Amazon Config, 请参阅put-configuration-recorder.

启用Amazon Config用Amazon CLI，请使用put-configuration-recorder、put-delivery-channel, 和start-configuration-recorder命令。

这些区域有：put-configuration-recorder命令会新建配置记录器，记录您选择的资源配置。这些区域有：put-delivery-channel命令会创建一个传输通道对象，将配置信息传输到 Amazon S3 存储桶和 Amazon SNS 主题。您账户中的每个区域都可以有一个配置记录器和一个传递通道。创建传送渠道后，start-configuration-recorder开始记录您选择的资源配置，您可以在Amazonaccount.

您可以指定记录器的名称和 IAM 角色的 Amazon 资源名称 (ARN)Amazon与账户关联的资源。默认情况下，Amazon Config在创建配置记录器时会自动分配名称 “default”。您不能更改分配的名称。

设置Amazon Config对于多账户多区域数据聚合Amazon CLI, 请参阅使用 设置聚合器AmazonCommand Line Interface. 需要为每个区域中的每个区域创建单独的配置记录器Amazon您想要记录配置项目的账户。

目录

put-configuration-recorder

您的put-configuration-recorder命令应类似于以下示例：

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default,roleARN=arn:aws:iam::123456789012:role/config-role --recording-group
 allSupported=true,includeGlobalResourceTypes=true
```

此命令使用 --recording-group 参数的以下选项：

- allSupported=true–Amazon Config将记录每种受支持类型的配置更改区域资源. Amazon Config 添加对新区域资源类型的支持后，它将自动开始记录该类型的资源。
- includeGlobalResourceTypes=true–Amazon Config将受支持类型的全局性资源包含在它所记录的资源中。Amazon Config 添加对新全球性资源类型的支持后，它将自动开始记录该类型的资源。

  在将此选项设置为 true 之前，您必须将 allSupported 选项设置为 true。

  如果您不希望包括全局性资源，请将此选项设置为 false，或者忽略此选项。

put-delivery-channel

要设置传送渠道，请使用put-delivery-channel命令：

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

deliveryChannel.json 文件指定了传递通道的属性：

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

此示例设置了以下属性：

- `name`— 传递通道的名称。默认情况下，Amazon Config 会向新的传递通道分配名称 `default`。

  您无法使用 `put-delivery-channel` 命令更新传递通道的名称。有关更改名称的步骤，请参阅 重命名传递通道 (p. 78)。
- `s3BucketName`— 存放的 Amazon S3 存储桶的名称Amazon Config可以提供配置快照和配置历史记录文件。

  如果您指定的存储桶属于其他 Amazon 账户，则该存储桶必须拥有向 Amazon Config 授予访问权限的策略。有关更多信息，请参阅 Amazon S3 存储桶的权限 (p. 221)。
- `snsTopicARN`— Amazon SNS 主题的 Amazon 资源名称 (ARN)Amazon Config发送有关配置更改的通知。

  如果您从其他账户选择主题，则该主题必须拥有授予 Amazon Config 访问权限的策略。有关更多信息，请参阅 Amazon SNS 主题的权限 (p. 225)。
- `configSnapshotDeliveryProperties`— Contains`deliveryFrequency`属性，此权限以设置频率Amazon Config提供配置快照。

start-configuration-recorder

要完成开启Amazon Config，请使用`start-configuration-recorder`命令：

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

检查那个Amazon Config已开启

在开启后Amazon Config，您可以使用Amazon CLI命令来检查Amazon Config正在运行那个Amazon Config已创建配置记录器和传输通道。您也可以确认 Amazon Config 是否已开始记录配置并向传递通道传递这些配置。

目录

检查是否已创建传递通道

使用`describe-delivery-channels`命令来检查您的 Amazon S3 存储桶和 Amazon SNS 主题是否已配置。

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-west-2:0123456789012:my-config-topic",
            "name": "my-delivery-channel",
            "s3BucketName": "my-config-bucket"
        }
    ]
}
```

当您使用 CLI、服务 API 或开发工具包配置传递通道且不指定名称时，Amazon Config 将自动分配“`default`”名称。

检查是否已创建配置记录器

使用describe-configuration-recorders命令来检查是否已创建配置记录器以及该配置记录器是否已代入了 IAM 角色。有关更多信息，请参阅 创建 IAM 角色 (p. 42)。

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

检查那个Amazon Config已开始记录

使用describe-configuration-recorder-status命令来检查Amazon Config已开始记录受支持的Amazon您账户中存在的资源。记录的配置会传递到指定的传递通道。

```
$ aws configservice describe-configuration-recorder-status
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "lastStopTime": 1414511624.914,
            "lastStartTime": 1414708460.276,
            "recording": true,
            "lastStatusChangeTime": 1414816537.148,
            "lastErrorMessage": "NA",
            "lastErrorCode": "400"
        }
    ]
}
```

`recording` 字段中的值 `true` 用于确认配置记录器已开始记录您的所有资源的配置。Amazon Config 采用 UTC 格式来记录时间。输出显示为 Unix 时间戳。

有关如何查找账户中的现有资源以及了解资源配置的信息，请参阅查看 Amazon 资源配置和历史记录 (p. 57)。

将 Amazon Config 与 Amazon 开发工具包配合使用

Amazon 软件开发工具包 (SDK) 可用于很多常用编程语言。每个软件开发工具包都提供 API、代码示例和文档，使开发人员能够更轻松地以其首选语言构建应用程序。

软件开发工具包文档
Amazon SDK for Java
Amazon SDK for JavaScript
Amazon SDK for .NET
Amazon SDK for PHP

软件开发工具包文档
Amazon SDK for Python (Boto3)
Amazon SDK for Ruby

使用Amazon Config控制台规则

Rules (规则) 页面提供了初始 Amazon 托管规则，您可以将这些规则添加到自己的账户。在设置之后，Amazon Config 根据您选择的规则来评估您的 Amazon 资源。您可以在设置之后更新规则和创建其他托管规则。

要查看 Amazon 托管规则的完整列表，请参阅 Amazon Config 托管规则的列表 (p. 123)。

例如，您可以选择cloudtrail-enabled规则，该规则将评估您的账户是否具有 CloudTrail 跟踪。如果您的账户没有跟踪，Amazon Config 会将资源类型以及规则标记为不合规。

在 Rules 页面上，可以执行以下操作：

- 在搜索字段中键入，以便按规则名称、描述或标签筛选结果。例如，键入 EC2 可返回评估 EC2 资源类型的规则，或者键入 periodic 可返回具有定期触发器的规则。键入“new”可搜索新添加的规则。有关触发器类型的更多信息，请参阅为 Amazon Config 规则指定触发器 (p. 122)。
- 选择一个规则，以查看其特定详细信息。您也可以通过选择旁边的箭头来按字母顺序对结果进行重新排序规则名称标签。
- 选择箭头图标可查看下一页规则。
- 查看最近添加的标记为New.
- 查看标签来确定规则所评估的资源类型以及规则是否具有定期触发器。

设置 Amazon Config 规则

1. 在 Rules 页面上，选择所需的规则。您可以自定义这些规则，并在设置之后将其他规则添加到您的账户。
2. 选择 Next（下一步）。
3. 在 Review 页面上，验证您的设置详细信息，然后选择 Confirm。

   Rules 页面在一个表中显示您的规则及其当前的合规性结果。在 根据规则完成对您的资源的评估前，每个规则的结果都显示为 Evaluating...Amazon Config。您可以使用刷新按钮更新结果。当 Amazon Config 完成评估时，您可以看到合规或不合规的规则和资源类型。有关更多信息，请参阅 查看配置合规性 (p. 63)。

   Note

   Amazon Config 仅评估它所记录的资源类型。例如，如果您将cloudtrail-enabled规则，但不要记录 CloudTrail 追踪资源类型，Amazon Config无法评估您账户中的跟踪是合规还是不合规。有关更多信息，请参阅 选择 Amazon Config 所记录的资源 (p. 73)。

您可以查看、编辑和删除现有规则。您还可以创建额外的 Amazon 托管规则或创建自己的规则。有关更多信息，请参阅 管理您的 Amazon Config 规则 (p. 204)。

将规则评估发送到Security Hub

在添加一个Amazon Config规则，您也可以将规则评估发送到Amazon Security Hub. 两者之间的整合Amazon Config和 Security Hub 允许您对规则评估以及其他错误配置和安全问题进行分类和修复。

将规则评估发送到Security Hub

要将规则评估发送到 Security Hub，您必须先设置Amazon Security Hub和Amazon Config，然后至少添加一个Amazon Config托管或自定义规则。在此之后，Amazon Config立即开始向 Security Hub 发送规则评估。Security Hub 丰富了规则评估并将其转换为Security Hub 调查结果。

有关此集成的更多信息，请参阅AvailableAmazon服务集成中的Amazon Security Hub用户指南。

查看 Amazon 资源配置和管理 Amazon Config

使用 Amazon Config 执行以下操作：

- 查看 Amazon Config 在您的账户中记录的所有资源。
- 自定义 Amazon Config 记录的资源类型。
- 在 Amazon Config 控制台和 Amazon CLI 中查看资源在特定时间段内的配置更改。
- 查看 Amazon 资源配置历史记录
- 查看 Amazon 资源合规性历史记录
- 查看所有通知Amazon Config发送到 Amazon SNS 主题。
- 修改 IAM 角色的设置
- 修改或删除您的传递通道

主题

区域支持

目前，以下区域中支持 Amazon Config：

区域名称	区域	Endpoint	协议
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS

区域名称	区域	Endpoint	协议
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Amazon GovCloud（美国东部）	us-gov-east–1	config。us-gov-east-1.amazonaws.com	HTTPS
Amazon GovCloud（美国西部）	us-gov-west–1	config。us-gov-west-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧洲（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧洲（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

查看 Amazon Config 控制面板

使用控制面板查看您的资源、规则及其合规性状态的概览，并可视化您的Amazon Config亚马逊的使用情况和成功指标CloudWatch. 此页面可帮助您快速识别您的前几个资源Amazon帐户，哪些规则或资源不合规，哪些流量驱动着你的Amazon Config使用情况以及工作流中发生故障的关键指标。

使用 Amazon Config 控制面板

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在左侧导航窗格中，选择控制面板.

目录

合规性和资源清单

安装完成后，Amazon Config会开始记录您指定的资源，然后根据您的规则对其进行评估。可能需要几分钟Amazon Config以显示您的资源、规则及其合规性状态。

Compliance status

合规性状态显示合规和不合规规则的数量以及合规和不合规的资源数量。根据对与之相关的规则的评估，资源是合规或不合规的。如果资源不符合规则的规范，则资源和规则将被标记为不合规。

要查看不合规的规则和资源列表，请选择不合规规则要么不合规的资源.

按不合规资源计数列出的不合规规则

按不合规资源计数列出的不合规规则按资源数量降序显示您的顶级不合规规则。选择一个规则以查看其详细信息、参数以及该特定规则范围内的资源。

有关不合规规规则的完整列表，请选择查看所有不合规规规则.

资源清单

资源清单显示以下项的资源的总数Amazon Config按资源数量和您的每种资源类型的计数降序记录Amazonaccount. 要打开某个资源类型的所有资源，请选择该资源类型以转到其资源清单页.

您可以使用下拉列表来指示要查看的资源总数。默认情况下，将其设置为查看所有资源，但是你可以将其更改为Amazon资源、第三方资源或自定义资源。

Note

这些区域有：评估您的Amazon使用 Config 规则配置资源消息可能会出现在控制面板出于以下原因：

- 您还没有设置Amazon Config适用于您的规则Amazonaccount. 您可以选择 Add rule 以转到 Rules 页面。
- Amazon Config 仍在按照您的规则评估您的资源。您可以刷新该页面来查看最新的评估结果。
- Amazon Config 根据您的规则评估您的资源，但没有在范围内找到任何资源。您可以在 Amazon ConfigSettings 页面中指定 要记录的资源。有关更多信息，请参阅 选择 Amazon Config 所记录的资源 (p. 73)。

Amazon Config用量指标和成功指标

你可以使用亚马逊CloudWatch中的控制面板Amazon Config控制台可视化Amazon Config使用情况和成功指标。

对于每个控制面板，您可以执行以下操作：

- 调整仪表板的时间范围以显示过去的数据1 小时、3 小时、12 小时、1 天、3 天，或者1 周.
- 选择Custom (自定义)，输入自定义时间范围：相对超过指定时间的时间或绝对两个日期之间的时间范围。您还可以更改时间格式以显示控制面板数据UTC（协调世界时）或本地时区（在您当前使用的计算机的操作系统中指定为本地时区的时区）。
- 使用丢弃箭头下一步刷新图标指定仪表板中的数据应该刷新的频率，或者关闭自动刷新。选择Off、10 秒、1 分钟、2 分钟、5 分钟，或者15 分钟以更改内部刷新。
- 选择添加到控制面板添加Amazon Config使用情况指标或Amazon Config您当前正在查看的成功指标Amazon Config控制面板到CloudWatch控制台。这将在CloudWatch控制台允许您在中创建新的自定义控制面板CloudWatch从你当前复制的信息Amazon Config使用情况指标或Amazon Config成功指标。

如果你想对这些指标执行额外的分析CloudWatch，选择指标在左侧导航窗格中CloudWatch控制台然后选择Amazon/配置. 有关您可以从CloudWatch控制台，请参阅使用 AmazonCloudWatch仪表板和使用AmazonCloudWatch指标中的CloudWatch用户指南。

Amazon Config用量指标

记录的配置项显示为每种资源类型或所有资源类型记录的配置项目数。配置项目代表point-in-time查看受支持的各种属性Amazon资源。有关配置项或支持的资源类型的更多信息，请参阅配置项和支持的资源类型.

您可以使用下拉列表选择要查看的资源类型。默认情况下，将其设置为查看所有资源类型。

Amazon Config成功指标

失败更改通知传输显示您的配送渠道向 Amazon SNS 主题发送失败的更改通知数量。更改通知会通知您有关您的配置状态的更改Amazon资源的费用。您可以使用ConfigStreamDeliveryInfo获取API`lastErrorCode`要么`lastErrorMessage`针对变更通知的最后一次尝试配送。有关更多信息，请参阅 。管理传递通道.

Config 历史导出失败显示导出到 Amazon S3 存储桶的失败的配置历史记录的数量。配置历史记录是指定资源在指定时间段的配置项的集合。有关配置记录的更多信息，请参阅配置历史.

配置记录器权限不足失败显示由于配置记录器的 IAM 角色策略权限不足而导致的权限访问尝试失败的次数。配置记录器在您的资源配置中检测更改，并将这些更改捕获为配置项。为了记录配置记录器来记录Amazon资源配置，它需要必要的 IAM 权限。有关更多信息，请参阅 。获取配置详细信息的 IAM 角色策略.

导出 Config 快照失败显示导出到 Amazon S3 存储桶的失败的配置快照的数量。配置快照是您账户中受支持资源的配置项的集合。有关配置快照的更多信息，请参阅配置快照.

查看 Amazon 资源配置和历史记录

您可以查看 Amazon Config 正在记录的您账户中的所有资源、某一资源在指定时间段内发生的配置更改及选定资源与所有相关资源之间的关系。您还可以查看时间线中显示的由 Amazon Config Rules 评估的资源的合规性状态更改。

主题

查找 Amazon Config 发现的资源

您可以使用 Amazon Config 控制台、Amazon CLI 和 Amazon Config API 来查找 Amazon Config 已清点或发现 的资源，包括已删除的资源和 Amazon Config 目前未记录的资源。Amazon Config 仅会发现受支持的资源类型。有关更多信息，请参阅 支持的资源类型 (p. 7)。

查找资源 (Amazon Config 控制台)

您可以使用资源类型或标签信息在 Amazon Config 控制台中查找资源。

查找资源

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在存储库的资源清单在页上，为您要查找的资源指定搜索选项：
   - 资源类别— 选择所有资源类别或将结果限制为仅限Amazon资源。
   - 资源类型— 选择所有资源类型或选择要筛选的资源。
   - 合规性— 选择按任何合规状态、合规或不合规状态进行筛选。
3. Amazon Config 列出与您的搜索选项匹配的资源。您可以查看有关资源的以下信息：
   - 资源标识符— 资源标识符可以是资源 ID，也可以是资源名称（如适用）。选择资源标识符链接以查看资源详细信息页面。
   - 资源类型— 列出资源的类型。
   - 合规性— 资源的状态Amazon Config按照您的规则评估。

     有关更多信息，请参阅 查看配置详细信息 (p. 59)。

查找资源 (Amazon CLI)

您可以使用 Amazon CLI 列出 Amazon Config 已发现的资源。

查找资源 (Amazon CLI)

- 使用 Amazon Configservice **`list-discovered-resources`** 命令：

  Example

```
$ aws configservice list-discovered-resources --resource-type "AWS::EC2::Instance"
        {
            "resourceIdentifiers": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-nnnnnnnn"
                }
            ]
```

```
        }
```

要查看响应中列出的某个资源的配置详细信息，请使用 `get-resource-config-history` 命令，并指定资源类型和 ID。有关此命令以及来自 Amazon Config 的响应的示例，请参阅查看配置历史记录 (p. 59)。

查找资源 (Amazon Config API)

您指定资源类型后，Amazon Config 将返回该类型资源的资源标识符列表。有关更多信息，请参阅 。ResourceIdentifier中的Amazon ConfigAPI 参考.

查找资源 (Amazon Config API)

- 使用ListDiscovered资源action.

要获取响应中列出的某个资源的配置详细信息，请使用 GetResourceConfigHistory 操作，并指定资源类型和 ID。

查看配置详细信息

您可以在 Amazon Config 控制台中查看配置、关系，以及资源的更改次数。您可以使用 Amazon CLI 查看资源的配置历史记录。

查看配置详细信息（控制台）

当你在资源清单页面上，选择资源标识符列中的资源名称或 ID 可查看资源的详细信息页面。详细信息页面提供了有关该资源的配置、关系和更改次数的信息。

要从资源详细信息页面访问资源时间线，请选择时间线按钮。资源时间线将更改捕获为`ConfigurationItems`在一段时间内针对特定资源。您可以按配置事件、合规性事件或CloudTrail事件。

查看配置详细信息 (Amazon CLI)

Amazon Config 记录的配置项会根据需要作为配置快照或配置流传递到指定的传递通道。您可以使用 Amazon CLI 来查看每个资源的配置项的历史记录。

查看配置历史记录

键入 `get-resource-config-history` 命令并指定资源类型和资源 ID，例如：

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup --
resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
```

```
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions\":
[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":[{\"userId
\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed\"}],
\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort\":65535,
\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default\",\"groupId
\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default\",
\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp\",\"fromPort\":-1,
\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"tcp\",\"fromPort
\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol
\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,\"userIdGroupPairs\":[],\"ipRanges\":
[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```


有关响应字段的详细解释，请参阅 Components of a Configuration Item (p. 24) 和 支持的资源类型 (p. 7)。

中的示例 Amazon EBS 配置历史记录Amazon Config

Amazon Config生成一组文件（其中每个文件均代表一个资源类型）并列出相应类型的资源的所有配置更改Amazon Config正在录制。Amazon Config将此以资源为中心的配置历史记录导出为您在启用时指定的 Amazon S3 存储桶中的对象Amazon Config. 每个资源类型的配置历史记录文件中包含自上一个历史记录文件传送完毕后检测到的该类型资源出现的更改。历史记录文件通常每六小时传送一次。

以下是 Amazon S3 对象内容的示例，其中描述了您的当前区域中所有 Amazon Elastic Block Store 卷的配置历史记录。Amazonaccount. 此账户中的卷包括 `vol-ce676ccc` 和 `vol-cia007c`。卷 `vol-ce676ccc` 自上一个历史记录文件传送完毕后有两项配置更改，而卷 `vol-cia007c` 只有一项更改。


```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
```

```
        "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
        "accountId": "12345678910",
        "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
        "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adb69edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04ad92281"
        ],
        "availibilityZone": "us-west-2b",
        "resourceType": "AWS::EC2::Volume",
        "resourceCreationTime": "2014-02-27T21:43:53.885Z",
        "tags": {},
        "relationships": [
            {
                "resourceId": "i-344c463d",
                "resourceType": "AWS::EC2::Instance",
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
            "snapshotId": "",
            "availabilityZone": "us-west-2b",
            "state": "in-use",
            "createTime": "2014-02-27T21:43:53.0885+0000",
            "attachments": [
                {
                    "volumeId": "vol-ce676ccc",
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "vol-ce676ccc",
        "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
        "accountId": "12345678910",
        "configurationItemCaptureTime": "2014-03-07T21:47:08.918Z",
        "configurationItemState": "3e660fdf-4e34-4f32-sseb-0ace5bf3d63a",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-ad229edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04w292281"
        ],
        "availibilityZone": "us-west-2b",
        "resourceType": "AWS::EC2::Volume",
        "resourceCreationTime": "2014-02-27T21:43:53.885Z",
        "tags": {},
```

```
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-cia007c",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-cia007c",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T20:47:08.918Z",
            "configurationItemState": "3e660fdf-4e34-4f88-sseb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adjhk8edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a67u292281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T20:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344e563d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-cia007c",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
```

```
                "createTime": "2014-02-27T20:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-cia007c",
                        "instanceId": "i-344e563d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

查看配置合规性

您可以使用 Amazon Config 控制台、Amazon CLI 或 Amazon Config API 查看您的规则及资源的合规性状态。

目录

查看合规性 (控制台)

查看合规性

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在 Amazon Web Services Management Console菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关支持的区域列表，请参阅。Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
3. 在导航窗格中，选择 Resources。在资源清单页面上，您可以按资源类别、资源类型和合规性状态进行筛选。选择包含删除的资源根据需要设置。该表显示了资源类型的资源标识符和该资源的资源合规性状态。资源标识符可以是资源 ID，也可以是资源名称。
4. 从资源标识符列中选择资源。
5. 选择资源时间线按钮。您可以按配置事件、合规性事件或者进行筛选CloudTrail事件。

   Note

   或者，在资源清单页面上，您可以直接选择资源名称。要从资源详细信息页面访问资源时间线，请选择资源时间线按钮。

此外，您还可以在 Resource inventory 页面查找您的资源，以查看其合规性。有关更多信息，请参阅 查找 Amazon Config 发现的资源 (p. 58)。

查看合规性 (CLI)

Example 查看合规性

要查看合规性，请使用以下任一 CLI 命令：

- 要查看您的每个规则的合规性状态，请使用 `describe-compliance-by-config-rule` 命令，如以下示例所示：

```
$ aws configservice describe-compliance-by-config-rule
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "instances-in-vpc"
        },
        {
            "Compliance": {
                "ComplianceType": "COMPLIANT"
            },
            "ConfigRuleName": "restricted-common-ports"
        },
...
```

  对于合规性类型为 `NON_COMPLIANT` 的每个规则，Amazon Config 将为 `CappedCount` 参数返回不合规资源的数量。

- 要查看 Amazon Config 根据特定规则评估的每个资源的合规性状态，请使用 `get-compliance-details-by-config-rule` 命令，如以下示例所示：

```
$ aws configservice get-compliance-details-by-config-rule --config-rule-
name ConfigRuleName{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1443610576.349,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-nnnnnnnn",
                    "ConfigRuleName": "ConfigRuleName"
                }
            },
            "ResultRecordedTime": 1443751424.969,
            "ConfigRuleInvokedTime": 1443751421.208,
            "ComplianceType": "COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1443610576.349,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-nnnnnnnn",
                    "ConfigRuleName": "ConfigRuleName"
                }
```

```
            },
            "ResultRecordedTime": 1443751425.083,
            "ConfigRuleInvokedTime": 1443751421.301,
            "ComplianceType": "NON_COMPLIANT"
        },
...
```

- 要查看每个特定类型的 Amazon 资源的合规性状态，请使用 describe-compliance-by-resource 命令，如以下示例所示：

```
$ aws configservice describe-compliance-by-resource --resource-type AWS::EC2::Instance
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-nnnnnnnn",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 1,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-nnnnnnnn",
            "Compliance": {
                "ComplianceType": "COMPLIANT"
            }
        },
...
```

- 要查看单个 Amazon 资源的合规性详细信息，请使用 get-compliance-details-by-resource 命令。

```
$ aws configservice get-compliance-details-by-resource --resource-type AWS::EC2::Instance
 --resource-id i-nnnnnnnn
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1443610576.349,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-nnnnnnnn",
                    "ConfigRuleName": "instances-in-vpc"
                }
            },
            "ResultRecordedTime": 1443751425.083,
            "ConfigRuleInvokedTime": 1443751421.301,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

查看合规性 (API)

Example 查看合规性

要查看合规性，请使用以下任一 API 操作：

- 要查看您的每个规则的合规性状态，请使用DescribeComplianceByConfigRuleaction.
- 要查看 Amazon Config 根据特定规则评估的每个资源的合规性状态，请使用 GetComplianceDetailsByConfigRule 操作。
- 要查看每个特定类型的 Amazon 资源的合规性状态，请使用 DescribeComplianceByResource 操作。
- 查看个人的合规性详细信息Amazon资源，请使用GetComplianceDetailsBy资源action. 详细信息包括：用于评估资源的 Amazon Config 规则有哪些、每个规则最后一次评估资源的时间，以及资源是否符合每个规则。

查看资源合规性历史时间线

Amazon Config 支持存储由 Amazon Config Rules 评估的资源的合规性状态更改。资源合规性历史记录以时间线的形式显示。时间线将特定资源在一段时间内的更改捕获为 `ConfigurationItems`。有关内容的信息`ConfigurationItem`，请参阅ConfigurationItem中的Amazon ConfigAPI 参考。

您可以选择加入或退出以记录中的所有资源类型Amazon Config. 如果您已选择记录所有资源类型，Amazon Config自动开始记录评估的资源合规性历史记录Amazon Config Rules. 默认情况下，Amazon Config 会记录所有受支持资源的配置更改。您也可以仅选择特定的资源合规性历史记录资源类型：`AWS::Config::ResourceCompliance`. 有关更多信息，请参阅 。选择哪些资源Amazon Config记录.

使用资源查看资源时间线

通过从资源清单页面中选择特定资源来访问资源时间线。

1. 选择资源从左侧导航窗格中选择。
2. 在资源清单页面上，您可以按资源类别、资源类型和合规性状态进行筛选。选择包含已删除的资源如果合适。

   该表显示了资源类型的资源标识符和该资源的资源合规性状态。资源标识符可以是资源 ID，也可以是资源名称。
3. 从资源标识符列中选择资源。
4. 选择资源时间轴按钮。您可以按配置事件、合规性事件或 CloudTrail 事件。

   Note

   或者，在资源清单页面上，您可以直接选择资源名称。要从资源详细信息页面访问资源时间线，请选择资源时间轴按钮。

使用规则查看资源时间线

通过从规则页面中选择特定规则来访问资源时间线。

1. 从左侧导航中选择 Rules (规则)。
2. 在 Rules (规则) 页面上，选择评估您的相关资源的规则。如果屏幕上未显示任何规则，请使用 Add rule (添加规则) 按钮来添加规则。
3. 在规则详细信息页面上，从已评估资源表中选择资源。
4. Select.资源时间轴按钮。此时将显示资源时间轴。

查询合规性历史记录

使用查询资源合规性历史记录 get-resource-config-history 使用资源类型`AWS::Config::ResourceCompliance`.

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ResourceCompliance --resource-id AWS::S3::Bucket/configrules-bucket
```

您应该可以看到类似于如下所示的输出内容：

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
     "relationshipName": "Is associated with "
    }
   ]
   "tags": {},
   "resourceType": "AWS::Config::ResourceCompliance",
   "resourceId": "AWS::S3::Bucket/configrules-bucket",
   "ConfigurationStateId": "1539799966921",
   "relatedEvents": [];
   "awsRegion": "us-west-2",
   "version": "1.3",
   "configurationItemMD5Hash": "",
   "supplementaryConfiguration": {},
   "configuaration": "{\"complianceType\":\"COMPLIANT\",\"targetResourceId\":\"configrules-
bucket\",\"targetResourceType\":\"AWS::S3::Bucket\",\configRuleList\":[{\"configRuleArn
\":\"arn:aws:config:us-west-2:AccountID:config-rule/config-rule-w1gogw\",\"configRuleId\":
\"config-rule-w1gogw\",\"configRuleName\":\"s3-bucket-logging-enabled\",\"complianceType\":
\"COMPLIANT\"}]}",

   "configurationItemStatus": "ResourceDiscovered",
   "accountId": "AccountID"
  }
 ]
}
```

将配置快照传送至 Amazon S3 存储桶

Amazon Config提供的配置快照Amazon那些资源Amazon Config将记录到您在配置传递通道时指定的 Amazon S3 存储桶。

主题

传送配置快照

Amazon Config在调用时生成配置快照DeliverConfig快照操作或者你运行Amazon CLI `deliver-config-snapshot`命令。Amazon Config将配置快照存储在您启用时指定的 Amazon S3 存储桶。Amazon Config.

键入 `deliver-config-snapshot` 命令，并指定在您配置传递通道时由 Amazon Config 分配的名称，例如：

```
$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
```

```
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}
```

来自 Amazon Config 的配置快照示例

下面是 Amazon Config 在配置快照中提供的信息示例。该快照描述了 Amazon Config 在当前区域中为您的 Amazon 账户记录的资源的相关配置，以及这些资源之间的关系。

Note

配置快照中可能会引用不支持的资源类型和资源 ID。

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
```

```
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "i-344c463d",
        "accountId": "12345678910",
        "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
        "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
        "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adb69edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04ad92281"
        ],
        "availibilityZone": "us-west-2b",
        "resourceType": "AWS::EC2::Instance",
        "resourceCreationTime": "2014-02-26T22:56:35.000Z",
        "tags": {
            "Name": "integ-test-1",
            "examplename": "examplevalue"
        },
        "relationships": [
            {
                "resourceId": "vol-ce676ccc",
                "resourceType": "AWS::EC2::Volume",
                "name": "Attached Volume"
            },
            {
                "resourceId": "vol-ef0e06ed",
                "resourceType": "AWS::EC2::Volume",
                "name": "Attached Volume",
                "direction": "OUT"
            },
            {
                "resourceId": "subnet-47b4cf2c",
                "resourceType": "AWS::EC2::SUBNET",
                "name": "Is contained in Subnet",
                "direction": "IN"
            }
        ],
        "configuration": {
            "instanceId": "i-344c463d",
            "imageId": "ami-ccf297fc",
            "state": {
                "code": 16,
                "name": "running"
            },
            "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
            "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
            "stateTransitionReason": "",
            "keyName": "configDemo",
            "amiLaunchIndex": 0,
            "productCodes": [],
            "instanceType": "t1.micro",
            "launchTime": "2014-02-26T22:56:35.0000+0000",
            "placement": {
                "availabilityZone": "us-west-2b",
                "groupName": "",
                "tenancy": "default"
            },
            "kernelId": "aki-fc8f11cc",
            "monitoring": {
                "state": "disabled"
```

```
    },
    "subnetId": "subnet-47b4cf2c",
    "vpcId": "vpc-41b4cf2a",
    "privateIpAddress": "172.31.21.63",
    "publicIpAddress": "54.218.4.189",
    "architecture": "x86_64",
    "rootDeviceType": "ebs",
    "rootDeviceName": "/dev/sda1",
    "blockDeviceMappings": [
        {
            "deviceName": "/dev/sda1",
            "ebs": {
                "volumeId": "vol-ef0e06ed",
                "status": "attached",
                "attachTime": "2014-02-26T22:56:38.0000+0000",
                "deleteOnTermination": true
            }
        },
        {
            "deviceName": "/dev/sdf",
            "ebs": {
                "volumeId": "vol-ce676ccc",
                "status": "attached",
                "attachTime": "2014-03-07T23:46:28.0000+0000",
                "deleteOnTermination": false
            }
        }
    ],
    "virtualizationType": "paravirtual",
    "clientToken": "aBCDe123456",
    "tags": [
        {
            "key": "Name",
            "value": "integ-test-1"
        },
        {
            "key": "examplekey",
            "value": "examplevalue"
        }
    ],
    "securityGroups": [
        {
            "groupName": "launch-wizard-2",
            "groupId": "sg-892adfec"
        }
    ],
    "sourceDestCheck": true,
    "hypervisor": "xen",
    "networkInterfaces": [
        {
            "networkInterfaceId": "eni-55c03d22",
            "subnetId": "subnet-47b4cf2c",
            "vpcId": "vpc-41b4cf2a",
            "description": "",
            "ownerId": "12345678910",
            "status": "in-use",
            "privateIpAddress": "172.31.21.63",
            "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
            "sourceDestCheck": true,
            "groups": [
                {
                    "groupName": "launch-wizard-2",
                    "groupId": "sg-892adfec"
                }
            ],
            "attachment": {
```

```
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

下一步是验证配置快照是否成功传送到了传递通道。

验证传送状态

键入`describe-delivery-channel-status` 命令以验 Amazon Config 是否已开始将配置传送到指定的传递通道，例如：

```
$ aws configservice describe-delivery-channel-status
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

对命令的响应会列出 Amazon Config 将配置传送到您的存储桶和主题时使用的所有三种传输格式的状态。

请查看 `lastSuccessfulTime` 中的 `configSnapshotDeliveryInfo` 字段。时间应与您上次请求传送配置快照的时间一致。

Note

Amazon Config使用 UTC 格式（协调世界时）记录时间。

查看 Amazon S3 存储桶中的配置快照

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
2. 在 Amazon S3 控制台中所有存储桶选择您的 Amazon S3 存储桶的名称。
3. 单击查看您的存储桶中的嵌套文件夹，找到快照 ID 与由命令返回的 ID 相匹配的 `ConfigSnapshot` 对象。下载并打开对象以查看配置快照。

   S3 存储桶还包含一个名为 `ConfigWritabilityCheckFile` 的空文件。Amazon Config 创建该文件的目的是验证服务是否能成功写入 S3 存储桶。

管理Amazon资源配置和历史记录

您可以随时更改您的 IAM 角色的设置并修改或删除您的传递通道 (即亚马逊简单存储服务存储桶和亚马逊简单通知服务主题)。您可以启动或停止与您的账户相关联的配置记录器，还可以自定义要记录哪些类型的资源。

主题

更新分配给的 IAM 角色Amazon Config

您可以更新所代入的 IAM 角色Amazon Config请随时联系。在更新 IAM 角色之前，请确保您已经创建了一个新的角色来取代旧角色。您必须将策略关联到新的角色，以授权 Amazon Config 记录配置并将其发送到传递通道。此外，请确保复制您的新 IAM 角色的 Amazon 资源名称 (ARN)。您在更新 IAM 角色时需要使用该名称。有关创建 IAM 角色并将所需策略附加到 IAM 角色的信息，请参阅创建 IAM 角色 (p. 42).

Note

要查找现有 IAM 角色的 ARN，请转至 IAM 控制台：https://console.aws.amazon.com/iam/. 在导航窗格中选择 Roles。然后选择所需角色的名称，并在 Summary 页面顶部找到对应的 ARN。

更新 IAM 角色

您可以使用Amazon Web Services Management Console或者Amazon CLI.

在支持规则的区域中更新 IAM 角色 (控制台)

如果您在支持 Amazon Config 规则的区域中使用 Amazon Config，请完成以下步骤。有关支持区域的列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在导航窗格中，选择 Settings (设置)。
3. 在Amazon Config角色在部分中，选择 IAM 角色：
   - 创建角色–Amazon Config创建具有所需权限的角色。对于 Role name (角色名称)，您可以自定义 Amazon Config 创建的名称。
   - 从您的账户选择一个角色— 对于Role name (角色名称)在账户中选择一个 IAM 角色。Amazon Config 将附加所需的策略。有关更多信息，请参阅 分配给的 IAM 角色权限Amazon Config (p. 218)。

     Note

     如果您希望按原样使用 IAM 角色，请选中该框。Amazon Config不会将策略附加到角色。
4. 选择 Save（保存）。

在不支持规则的区域中更新 IAM 角色 (控制台)

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在存储库的资源清单页面上，选择设置图标 (⚙)。
3. 选择 Continue (继续)。
4. 在Amazon Config正在申请读取资源配置的权限页面上，选择详细信息.
5. 在角色摘要部分中，选择 IAM 角色：
   - 如果您希望创建角色，请为IAM 角色，选择创建新的 IAM 角色. 然后为键入名称角色名称.
   - 如果您想使用某个现有角色，对于 IAM Role，请选择现有角色。然后，对于策略名称，选择一个可用策略，或通过选择来创建策略创建新的角色策略.
6. 选择 Allow。

更新 IAM 角色 (Amazon CLI)

- 使用 `put-configuration-recorder` 命令并指定新角色的 Amazon 资源名称 (ARN)：

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

选择 Amazon Config 所记录的资源

Amazon Config 将持续检测任何受支持类型的资源的创建、更改或删除时间。Amazon Config 会将这些事件记录为配置项。您可以自定义Amazon Config将记录所有受支持类型的资源的更改，或仅记录与您相关的资源的更改。要了解 Amazon Config 可记录的资源类型，请参阅 支持的资源类型 (p. 7)。

记录所有受支持的资源类型

默认情况下，Amazon Config 会记录在 运行区域中发现的所有受支持类型的区域性资源Amazon Config的配置更改。区域性资源与某个区域相关联，且仅可在该区域中使用。区域性资源的示例为 EC2 实例和 EBS 卷。

您还可以让 Amazon Config 记录受支持类型的全局性资源。全局性资源不与特定区域相关联，并且可在所有区域使用。全局资源类型Amazon ConfigIAM 用户、组、角色和客户托管策略将受支持的策略包含在客户托管策略中。

Important

已载入的全局资源类型Amazon Config2022 年 2 月之后的录音将仅在该服务的所在区域录制用于商业分区Amazon GovCloud （美国西部）for the GovCloud 分区。您只能在其主区域查看这些新的全局资源类型的配置项，并且Amazon GovCloud （美国西部）。
2022 年 2 月之前加入的受支持的全局资源类型，例如`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、`AWS::IAM::User`保持不变，并且他们将继续在中启用的所有区域提供配置物品Amazon Config. 此更改只会影响 2022 年 2 月之后加入的新全球资源类型。

主页 2022 年 2 月后加入的全球资源类型的地区

Amazon 服务	资源类型值	主区域
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	美国东部（弗吉尼亚州北部）区域
Amazon Global Accelerator	`AWS::GlobalAccelerator::Listener`	美国西部（俄勒冈州）区域
	`AWS::GlobalAccelerator::EndpointGroup`	美国西部（俄勒冈州）区域
	`AWS::GlobalAccelerator::Accelerator`	美国西部（俄勒冈州）区域

记录特定的资源类型

如果您不希望 Amazon Config 记录所有支持资源的更改，则可以对其进行自定义，以使其仅记录特定类型的资源更改。Amazon Config 记录您指定的资源类型的配置更改，包括这类资源的创建和删除。

如果未记录某个资源，Amazon Config 将仅记录该资源的创建和删除，而不会提供其他详细信息，且您无需支付任何费用。当某个未记录资源被创建或删除时，Amazon Config 将发送通知，并在资源详细信息页面显示该事件。在未记录资源的详细信息页面上，大多数配置详细信息的值为 null，且不会显示关于关系和配置更改的信息。

由于未记录资源的数据缺失，因此 Amazon Config 为已记录资源提供的关系信息不受限制。如果某个已记录资源与未记录资源相关联，则已记录资源的详细信息页面会提供相应的关系信息。

您可以随时使 Amazon Config 停止记录某个类型的资源。在 Amazon Config 停止记录某个资源后，它会保留之前捕获的配置信息，并且您可继续访问此类信息。

Amazon Config 规则可用于仅评估 Amazon Config 记录的那些资源的合规性。

选择资源 (控制台)

您可以使用 Amazon Config 控制台选择 Amazon Config 记录的资源类型。

选择资源

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 打开 Settings 页面：
   - 如果您在支持 Amazon Config 规则的区域中使用 Amazon Config，请在导航窗格中选择 Settings (设置)。有关支持的区域列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
   - 否则，请选择设置图标 (⚙) 在资源清单页.
3. 在 Resource types to record (要记录的资源类型) 部分中，指定您希望 Amazon Config 记录的 Amazon 资源的类型：

- 所有资源–Amazon Config将所有受支持的资源包含在以下选项中：
  - 记录该区域支持的所有资源–Amazon Config将记录每种受支持类型的区域性资源 的配置更改。Amazon Config 添加对新区域资源类型的支持后，它将自动开始记录该类型的资源。
  - 包含全球性资源–Amazon Config将受支持类型的全局性资源包含在它记录的资源（例如，IAM 资源）中。Amazon Config 添加对新全球性资源类型的支持后，它将自动开始记录该类型的资源。
- 特定类型–Amazon Config仅记录这些类型的配置更改Amazon您指定的资源。

4. 保存您的更改：

   - 如果您在支持 Amazon Config 规则的区域中使用 Amazon Config，请选择 Save (保存)。
   - 否则，请选择 Continue。在Amazon ConfigConfig 正在请求读取资源配置的权限页面上，选择Allow（允许）.

选择资源 (Amazon CLI)

您可以使用 Amazon CLI 选择您希望 Amazon Config 记录的资源类型。为此，您可以创建一个配置记录器，以记录您在记录组中指定的资源类型。在记录组中，您可以指定要记录所有受支持类型的资源，还是特定类型的资源。

选择所有受支持的资源

1. 使用以下 `put-configuration-recorder` 命令：

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default,roleARN=arn:aws:iam::123456789012:role/config-role --recording-group
 allSupported=true,includeGlobalResourceTypes=true
```

   此命令使用 `--recording-group` 参数的以下选项：

   - `allSupported=true`–Amazon Config将记录每种受支持类型的配置更改区域资源. Amazon Config 添加对新区域资源类型的支持后，它将自动开始记录该类型的资源。
   - `includeGlobalResourceTypes=true`–Amazon Config将受支持类型的全局性资源包含在它所记录的资源中。Amazon Config 添加对新全球性资源类型的支持后，它将自动开始记录该类型的资源。

     在将此选项设置为 `true` 之前，您必须将 `allSupported` 选项设置为 `true`。

     如果您不希望包括全局性资源，请将此选项设置为 `false`，或者忽略此选项。

2. (可选) 要验证您的配置记录器是否拥有您所需的设置，请使用以下 `describe-configuration-recorders` 命令：

```
$ aws configservice describe-configuration-recorders
```

   以下为响应示例：

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role",
            "name": "default"
        }
```

```
    ]
}
```

选择特定类型的资源

1. 使用 Amazon Configservice put-configuration-recorder 命令，并通过 --recording-group 选项传递一个或多个资源类型，如以下示例所示：

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default,roleARN=arn:aws:iam::012345678912:role/myConfigRole --recording-
group file://recordingGroup.json
```

   recordingGroup.json 文件指定了 Amazon Config 将记录的资源类型：

```
{
  "allSupported": false,
  "includeGlobalResourceTypes": false,
  "resourceTypes": [
    "AWS::EC2::EIP",
    "AWS::EC2::Instance",
    "AWS::EC2::NetworkAcl",
    "AWS::EC2::SecurityGroup",
    "AWS::CloudTrail::Trail",
    "AWS::EC2::Volume",
    "AWS::EC2::VPC",
    "AWS::IAM::User",
    "AWS::IAM::Policy"
  ]
}
```

   您必须将 resourceTypes 和 allSupported 选项设置为 false 或者忽略它们，才可以为 includeGlobalResourceTypes 键指定资源类型。

2. (可选) 要验证您的配置记录器是否拥有您所需的设置，请使用以下 describe-configuration-recorders 命令：

```
$ aws configservice describe-configuration-recorders
```

   以下为响应示例：

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": false,
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ],
                "includeGlobalResourceTypes": false
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role",
```

```
            "name": "default"
        }
    ]
}
```

管理传递通道

由于 Amazon Config 会持续记录您的 Amazon 资源发生的更改，因此，它会通过传递通道 发送通知和更新后的配置状态。您可以管理传递通道，从而控制 Amazon Config 在哪里发送配置更新。

每个 Amazon 账户每个区域只能有一个传递通道，且使用 Amazon Config 时必须使用传递通道。

何时Amazon Config检测到资源的配置更改，且通知超过 Amazon SNS 允许的最大大小，此通知会包含配置项的简短摘要。您可以在中指定的 Amazon S3 存储桶位置查看完整通知。`s3BucketLocation`字段中返回的子位置类型。有关更多信息，请参阅 。示例过大配置项变更通知.

> Note
>
> Amazon Config支持Amazon KMS使用的 Amazon S3 存储桶的加密Amazon Config 您可以提供Amazon Key Management Service(Amazon KMS) 密钥或别名 Amazon Resource Name (ARN)，以加密传输至 Amazon Simple Storage Service (Amazon S3) 存储桶的数据。默认情况下，Amazon Config将配置历史记录和快照文件传送到 Amazon S3 存储桶，并使用 S3 AES-256 服务器端加密 SSE-S3 对静态数据进行加密。但是，如果你提供Amazon Config用你的 KMS 密钥或别名 ARN，Amazon Config使用该 KMS 密钥而不是 AES-256 加密。
> Amazon Config不支持启用对象锁定的 Amazon S3 存储桶的传输通道。有关更多信息，请参阅 S3 对象锁定的工作原理。

更新传递通道

更新传递通道时，您可以设置以下选项：

- 向其传输的 Amazon S3 存储桶Amazon Config发送配置快照和配置历史记录文件。
- 多久Amazon Config向 Amazon S3 存储桶传输配置快照。
- 其访问的 Amazon SNS 主题Amazon Config发送有关配置更改的通知。

更新传递通道 (控制台)

- 您可以使用Amazon Config控制台为您的传递通道设置 Amazon S3 存储桶和 Amazon SNS 主题。有关管理这些设置的步骤，请参阅 使用控制台设置 Amazon Config (p. 27)。

  控制台不提供用于重命名传递通道、设置配置快照频率或删除传递通道的选项。要完成这些任务，您必须使用 Amazon CLI、Amazon Config API 或某个 Amazon 开发工具包。

更新传递通道 (Amazon CLI)

1. 使用 `put-delivery-channel` 命令：

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

   deliveryChannel.json 文件指定了传递通道的属性：

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
```

```
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

此示例设置了以下属性：

- `name`— 传递通道的名称。默认情况下，Amazon Config 会向新的传递通道分配名称 `default`。

  您无法使用 `put-delivery-channel` 命令更新传递通道的名称。有关更改名称的步骤，请参阅 重命名传递通道 (p. 78)。
- `s3BucketName`— 向其访问的 Amazon S3 存储桶的名称。Amazon Config传输配置快照和配置历史记录文件。

  如果您指定的存储桶属于其他 Amazon 账户，则该存储桶必须拥有向 Amazon Config 授予访问权限的策略。有关更多信息，请参阅 Amazon S3 存储桶的权限 (p. 221)。
- `snsTopicARN`— 向其访问的 Amazon SNS 主题的 Amazon 资源名称 (ARN)Amazon Config发送有关配置更改的通知。

  如果您从其他账户选择主题，则该主题必须拥有授予 Amazon Config 访问权限的策略。有关更多信息，请参阅 Amazon SNS 主题的权限 (p. 225)。
- `configSnapshotDeliveryProperties`— 包含`deliveryFrequency`属性，它设置频率Amazon Config传输配置快照。

2. (可选) 您可以使用 `describe-delivery-channels` 命令验证传递通道设置是否已更新：

```
$ aws configservice describe-delivery-channels
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

重命名传递通道

要更改传递通道的名称，您必须删除该传递通道，然后使用所需名称创建一个新传递通道。在删除传递通道之前，您必须暂时停止配置记录器。

Amazon Config 控制台不提供用于删除传递通道的选项，因此，您必须使用 Amazon CLI、Amazon Config API 或某个 Amazon 开发工具包。

重命名传递通道 (Amazon CLI)

1. 使用 `stop-configuration-recorder` 命令停止配置记录器：

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

2. 使用 `describe-delivery-channels` 命令，并记下您的传递通道属性：

```
$ aws configservice describe-delivery-channels
```

```
{
    "DeliveryChannels": [
        {
            "configSnapshotDeliveryProperties": {
                "deliveryFrequency": "Twelve_Hours"
            },
            "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

3. 使用 delete-delivery-channel 命令删除传递通道：

```
$ aws configservice delete-delivery-channel --delivery-channel-name default
```

4. 使用 put-delivery-channel 命令以所需名称创建传递通道：

```
$ aws configservice put-delivery-channel --delivery-channel file://deliveryChannel.json
```

deliveryChannel.json 文件指定了传递通道的属性：

```
{
    "name": "myCustomDeliveryChannelName",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-2:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

5. 使用 start-configuration-recorder 命令恢复记录：

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

管理配置记录器

Amazon Config 使用配置记录器 在您的资源配置中检测更改，并将这些更改捕获为配置项。您必须先创建配置记录器，然后 Amazon Config 才可以跟踪资源配置。

如果您使用控制台或 Amazon CLI 设置 Amazon Config，则 Amazon Config 会自动为您创建并启动配置记录器。有关更多信息，请参阅 开始使用 Amazon Config (p. 27)。

默认情况下，配置记录器会记录 Amazon Config 运行的区域内所有受支持的资源。您可以创建一个自定义配置记录器，仅记录您指定的资源类型。有关更多信息，请参阅 选择 Amazon Config 所记录的资源 (p. 73)。

当 Amazon Config 开始记录配置时，我们就会向您收取服务使用费。有关定价信息，请参阅 Amazon Config 定价。要控制成本，您可以通过停止配置记录器来停止记录。停止记录后，您可以继续访问已记录的配置信息。您将不用支付 Amazon Config 使用费，除非您恢复记录。

当您启动配置记录器时，Amazon Config 会使用您账户中的所有 Amazon 资源的清单。

管理配置记录器 (控制台)

您可以使用 Amazon Config 控制台终止或启动配置记录器。

停止或启动配置记录器

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在导航窗格中，选择 Settings (设置)。
3. 停止或启动配置记录器：
   - 如果您要停止记录，请选择 Recording is on 下的 Turn off。系统提示时，选择Continue.
   - 如果您要开始记录，请选择 Recording is off (记录已关闭) 下的 Turn on (开启)。系统提示时，选择Continue.

管理配置记录器 (Amazon CLI)

您可以使用 Amazon CLI 停止或启动配置记录器。您还可以使用重命名或删除配置记录器。Amazon CLI，Amazon ConfigAPI，或者其中一个Amazon开发工具包。以下步骤可帮助您使用 Amazon CLI。

停止配置记录器

- 使用 `stop-configuration-recorder` 命令：

```
$ aws configservice stop-configuration-recorder --configuration-recorder-
name configRecorderName
```

启动配置记录器

- 使用 `start-configuration-recorder` 命令：

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

重命名配置记录器

要更改配置记录器的名称，您必须删除该配置记录器，然后使用所需名称创建一个新配置记录器。

1. 使用 `describe-configuration-recorders` 命令查找当前配置记录器的名称：

```
$ aws configservice describe-configuration-recorders
{
    "ConfigurationRecorders": [
        {
            "roleARN": "arn:aws:iam::012345678912:role/myConfigRole",
            "name": "default"
        }
    ]
}
```

2. 使用 `delete-configuration-recorder` 命令删除当前配置记录器：

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

3. 使用 `put-configuration-recorder` 命令创建具有所需名称的配置记录器：

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=configRecorderName,roleARN=arn:aws:iam::012345678912:role/myConfigRole
```

4. 使用 `start-configuration-recorder` 命令恢复记录：

```
$ aws configservice start-configuration-recorder --configuration-recorder-
name configRecorderName
```

删除配置记录器

- 使用 `delete-configuration-recorder` 命令：

```
$ aws configservice delete-configuration-recorder --configuration-recorder-name default
```

记录托管实例的软件配置

您可以使用Amazon Config记录 Amazon EC2 实例和本地服务器的软件清单变更。这样您就可以了解到软件配置的变更历史。例如，当托管 Windows 实例安装了新的 Windows 更新时，Amazon Config 会记录变更情况并将其发送到您的传递通道，这样您就可以收到变更通知。借助 Amazon Config，您可以看到托管实例何时安装了 Windows 更新，以及它们随时间推移的变化情况。

您必须完成以下步骤来记录软件配置变更：

- 在 Amazon Config 中打开对托管实例清单资源类型的记录。
- 将 EC2 和本地服务器配置为托管实例在Amazon Systems Manager. 托管实例是已配置为与 Systems Manager 一起使用的机器。
- 使用 Systems Manager 清单功能启动收集托管实例的软件清单。

> **Note**
>
> Systems Manager 现在支持为创建配置项非托管实例
> 非托管实例的配置项目将具有补充配置`Key: “InstanceStatus”`和`Value: “Unmanaged”`.
> 非托管实例的配置项目将不会收到其他更新
> 要接收其他更新，配置项目必须是托管实例。

您也使用 Amazon Config 规则监控软件配置变更，并在变更符合或违反您的规则时获得通知。例如，如果您创建了一条规则，来检查托管实例是否安装了特定应用程序，那么如果某个实例未安装该应用程序，Amazon Config 会将这个实例标记为违反了您的规则。有关 Amazon Config 托管规则的列表，请参阅Amazon Config 托管规则的列表 (p. 123)。

在 Amazon Config 中启用软件配置变更的记录：

1. 在 Amazon Config 中记录所有支持的资源类型，或选择性地记录托管实例清单资源类型。有关更多信息，请参阅 选择 Amazon Config 所记录的资源 (p. 73)。
2. 启动具有 Systems Manager 的实例配置文件的实例配置文件，其中包含AmazonsSMManagedInstance核心实例托管策略。此 Amazon 托管策略使实例能够使用 Systems Manager 服务核心功能。

   有关可添加到 Systems Manager 的实例配置文件的其他策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南.

   > **Important**
   >
   > SSM Agent 是必须安装在托管实例上的 Amazon 软件，以便在云中与 Systems Manager 进行通信。如果您的 EC2 实例是从 AMI 为以下一种操作系统创建的，则会预装代理：
   >
   > - 2016 年 11 月或之后发布的 Windows Server 2003-2012 R2 AMI
   > - Windows Server 2016 和 2019

- Amazon Linux
- Amazon Linux 2
- Ubuntu Server 16.04
- Ubuntu Server 18.04

在不是从预装代理的 AMI 上创建的 EC2 实例上，必须手动安装代理。有关信息，请参阅中的以下主题：Amazon Systems Manager用户指南：

- 在适用于 Windows Server 的 EC2 实例上安装和配置 SSM Agent
- 在适用于 Linux 的 EC2 实例上安装和配置 SSM Agent

3. 按照中所述启动库存收集配置清单收集中的Amazon Systems Manager用户指南. Linux 和 Windows 实例的步骤相同。

   Amazon Config 可以记录以下清单类型的配置变更：

   - 应用程序— 托管实例的应用程序列表，例如防病毒软件。
   - Amazon组件— 列表Amazon托管实例的组件，例如Amazon CLI开发工具包。
   - 实例信息— 实例信息，例如操作系统名称和版本、域和防火墙状态。
   - 网络配置— 配置信息，例如 IP 地址、网关和子网掩码。
   - Windows 更新— 托管实例的 Windows 更新列表（仅适用于 Windows 实例）。

   Note

   Amazon Config 目前不支持记录自定义清单类型。

清单收集是众多 Systems Manager 功能的一种，这些功能分为类别。运营管理、操作 & 更改、实例和节点，和共享资源. 有关更多信息，请参阅 。什么是 Systems Manager？和Systems Manager 功能中的Amazon Systems Manager用户指南.

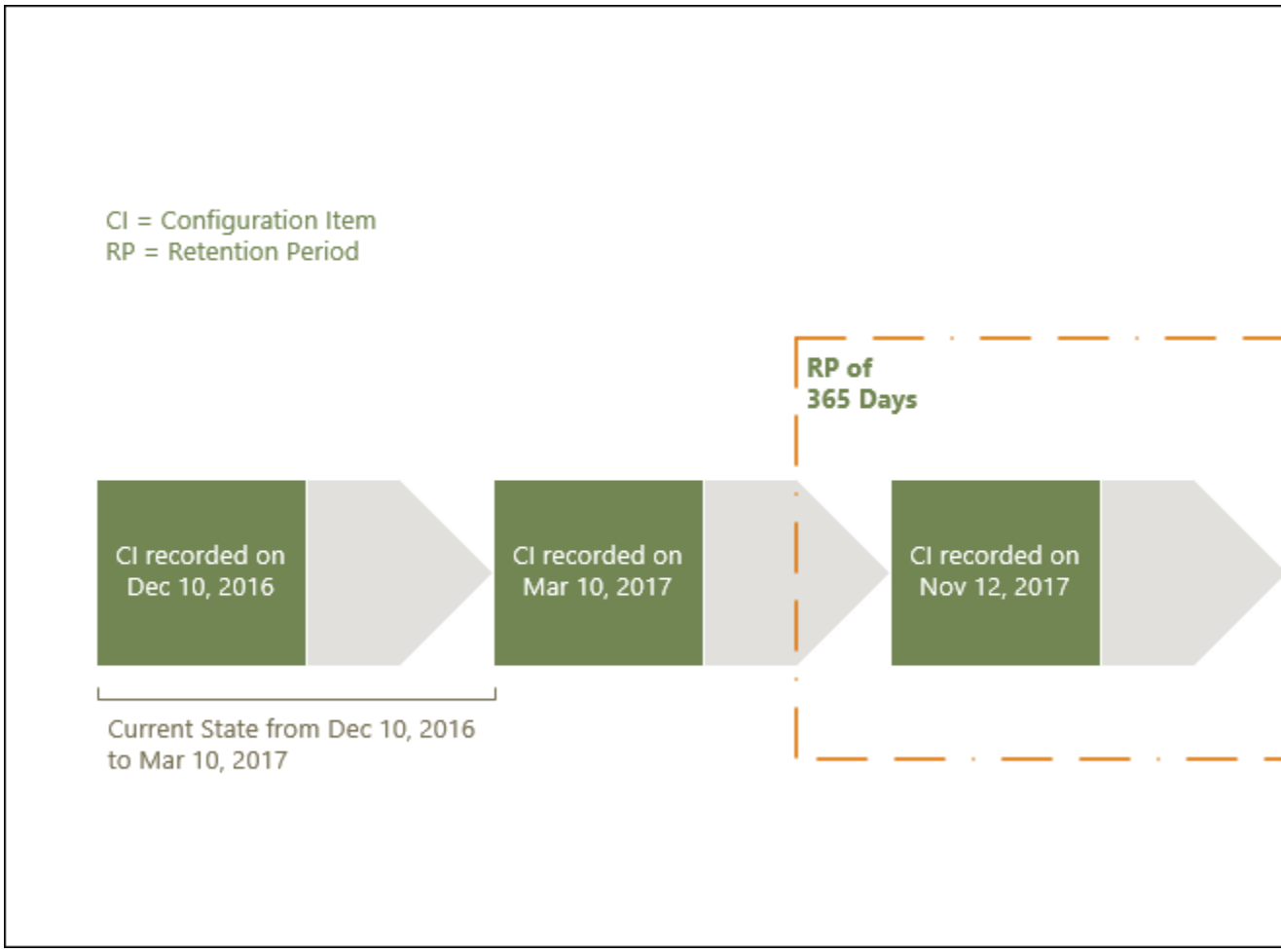
删除Amazon Config数据

Amazon Config通过为指定保留期来删除数据`ConfigurationItems`. 当您指定了保留期，Amazon Config保留您的`ConfigurationItems`在该指定时间内。您可以选择介于最少 30 天和最多 7 年（2557 天）之间的保留期。Amazon Config 会删除超过您指定的保留期的数据。如果您未指定保留期，Amazon Config 将继续在默认保留期 7 年（2557 天）内存储 `ConfigurationItems`。当记录功能打开时，资源的当前状态是 `ConfigurationItem` 被记录，直到记录下一个更改（新的 `ConfigurationItem`）。

为了理解保留期的行为，我们来看一下时间表。

- 当记录功能打开时，资源的当前状态始终存在，无法删除，无论记录 `ConfigurationItem` 的日期如何都是如此。
- 当 Amazon Config 记录新的 `ConfigurationItems` 时，之前的 `ConfigurationItems` 会被删除，具体取决于指定的保留期。

在以下时间表中，Amazon Config 会在以下日期记录 `ConfigurationItems`。针对此时间表的用途，今天表示为 2018 年 5 月 24 日。



下表说明了 Amazon Config 时间表上显示的 `ConfigurationItems` 是基于选定的保留期。

保留周期	在时间表上显示的配置项	说明
30 天	2017 年 12 月 12 日	资源的当前状态从 2017 年 12 月 12 日开始（`ConfigurationItem` 在那时被记录），并且直到今天（2018 年 5 月 24 日）有效。当记录功能打开时，当前状态始终存在。
365 天	2017 年 12 月 12 日；2017 年 11 月 12 日以及 2017 年 3 月 10 日	保留期显示当前状态 2017 年 12 月 12 日以及之前的 `ConfigurationItems` 2017 年 11 月 12 日以及 2017 年 3 月 10 日。 这些区域有：`ConfigurationItem`2017 年 3 月 10 日的显示在时间表上，因为该配置状态表示当前状态 365 天前。

在您指定保留期后，Amazon Config API 便不再返回表示状态超过指定保留期的 `ConfigurationItems`。

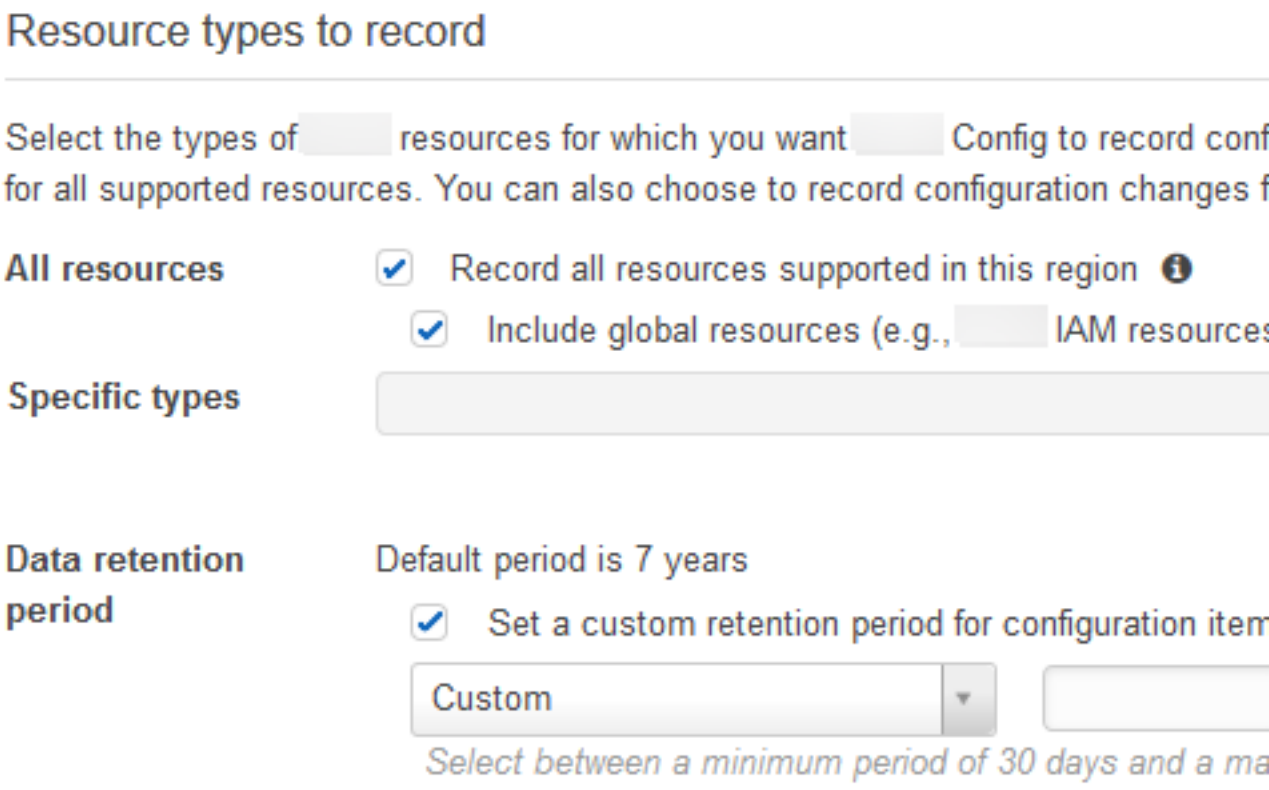
Note

- 如果记录功能已关闭，则 Amazon Config 无法记录您的 `ConfigurationItems`。
- Amazon Config无法录制你的`ConfigurationItems`如果您的 IAM 角色被破坏。

在 Amazon Web Services Management Console 中设置数据保留期

在 Amazon Web Services Management Console 中，如果您不选择数据保留期，则默认保留期为 7 年或 2557 天。

要为配置项设置自定义数据保留期，请选中该复选框。您可以选择 1 年、3 年、5 年或自定义期间。对于自定义期间，请输入介于 30 和 2557 天之间的天数。



记录第三方资源的配置

记录第三方资源或自定义资源类型的配置，例如本地服务器、SaaS 监控工具和版本控制系统（例如：GitHub)。您可以使用 Amazon Config 控制台和 API，将第三方资源的配置数据发布到 Amazon Config 中并查看和监控资源清单及配置历史记录。现在，您可以使用 Amazon Config 管理所有资源，并使用 Amazon Config 规则评估资源配置是否符合最佳实践。您还可以创建 Amazon Config 规则或一致性包，以根据最佳实践、内部策略和监管策略评估这些第三方资源。

Note

此功能仅在重新设计的 Amazon Config 控制台中可用。
如果您已将 Amazon Config 配置为记录所有资源类型，则系统会自动在 Amazon Config 中将通过 Amazon CloudFormation 管理（即创建/更新/删除）的第三方资源作为配置项目进行跟踪。

先决条件：必须使用注册第三方资源或自定义资源类型Amazon CloudFormation.

主题

第 1 步：设置开发环境

安装和配置 Amazon CloudFormation Amazon CLI。Amazon CLI 允许您建模和注册自定义资源。有关更多信息，请参阅 。自定义资源和什么是？CloudFormation命令行界面？.

第 2 步：为资源建模

创建符合资源类型配置的资源提供程序架构，并验证该架构。

1. 使用 `init` 命令创建资源提供程序项目并生成所需的文件。

```
$ cfn init
Initializing new project
```

2. `init` 命令将启动一个向导，引导您完成项目的设置，包括指定资源名称。在此演练中，指定 `MyCustomNamespace::Testing::WordPress`。

```
Enter resource type identifier (Organization::Service::Resource):
 MyCustomNamespace::Testing::WordPress
```

3. 输入资源的包名称。

```
Enter a package name (empty for default 'com.custom.testing.wordpress'):
 com.custom.testing.wordpress
Initialized a new project in /workplace/user/custom-testing-wordpress
```

Note

为了确保正确解决任何项目依赖项，您可以在 Maven 支持的情况下将生成的项目导入 IDE 中。
例如，如果您使用 IntelliJ IDEA，则需要执行以下操作：

- 从File (文件)选择菜单，选择New，然后选择来自现有来源的项目.
- 导航到项目目录
- 在导入项目对话框中，选择从外部模型导入项目然后选择玛文.

- 选择下一步并接受任何默认值以完成导入项目。

4. 打开包含您资源的架构的 mycustomnamespace-testing-wordpress.json 文件。将以下架构复制并粘贴到 mycustomnamespace-testing-wordpress.json 中。

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
      "description": "A name associated with the website.",
      "type": "string",
      "pattern": "^[a-zA-Z0-9]{1,219}\\Z",
      "minLength": 1, "maxLength": 219
    },
    "SubnetId": {
      "description": "A subnet in which to host the website.",
      "pattern": "^(subnet-[a-f0-9]{13})|(subnet-[a-f0-9]{8})\\Z",
      "type": "string"
    },
    "InstanceId": {
      "description": "The ID of the instance that backs the WordPress site.",
      "type": "string"
    },
    "PublicIp": {
      "description": "The public IP for the WordPress site.",
      "type": "string"
    }
  },
  "required": [ "Name", "SubnetId" ],
  "primaryIdentifier": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "readOnlyProperties": [ "/properties/PublicIp", "/properties/InstanceId" ],
  "additionalProperties": false
}
```

5. 验证架构。

```
$ cfn validate
```

6. 更新资源提供程序包中自动生成的文件以查看资源提供程序架构更新。启动资源提供程序项目后，Amazon CLI 为资源提供程序生成支持文件和代码。重新生成代码以查看更新的架构。

```
$ cfn generate
```

> **Note**
>
> 在使用 Maven 时，作为构建过程的一部分`generate`命令会在编译代码之前自动运行。因此，你的更改永远不会与生成的代码失去同步。
> 请注意CloudFormationCLI 必须位于 maven/ 系统可以找到的位置。有关更多信息，请参阅 。为开发扩展设置环境.

有关整个过程的更多信息，请参阅为在中使用建模资源提供程序Amazon CloudFormation.

第 3 步：生成构件

为生成构件，运行以下命令`cfn submit`.

```
$ mvn package
```

第 4 步：注册您的资源

Amazon Config 不需要资源提供程序的处理程序为您的资源执行配置跟踪。运行以下命令来注册您的资源。

```
$ cfn submit
```

有关更多信息，请参阅注册资源提供程序以在 Amazon CloudFormation 模板中使用。

第 5 步：发布资源配置

确定的配置MyCustom命名空间# 测试#WordPress.

```
{
  "Name": "MyWordPressSite",
  "SubnetId": "subnet-abcd0123",
  "InstanceId": "i-01234567",
  "PublicIp": "my-wordpress-site.com"
}
```

从 Amazon CloudFormation `DescribeType` 中确定架构版本 ID。

在 Amazon Config 中，查看是否接受了此资源配置。要评估合规性，您可以编写使用此资源的 Amazon Config 规则。有关更多信息，请参阅使用记录和删除第三方资源的配置状态AmazonCLI.

可选：要自动记录配置，请实施定期配置收集器或基于更改的配置收集器。

使用记录和删除第三方资源的配置状态Amazon CLI

Amazon CLI 是用于管理 Amazon 服务的统一工具。如果您仅使用一种工具进行下载和配置，则可通过命令行控制多个 Amazon 服务并使用脚本来自动执行这些服务。

安装Amazon CLI在本地计算机上，请参阅安装Amazon CLI中的Amazon CLI用户指南.

如有必要，请键入 `aws configure` 以配置 Amazon CLI。

主题

记录配置项

使用以下过程记录第三方资源或自定义资源类型的配置项：

确保您将资源类型 `MyCustomNamespace::Testing::WordPress` 注册到与其匹配的架构。

1. 打开命令提示符或终端窗口。
2. 键入以下命令：

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-id
 00000001 --configuration  '{
  "Id": "resource-001",
```

```
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

Note

正如类型架构中所定义的那样，`writeOnlyProperties`将在记录之前从配置中删除Amazon Config. 这意味着当通过读取 API 获取配置时，这些值将不存在。有关`writeOnlyProperties`请参阅架构资源类型.

使用阅读配置项Amazon ConfigAPI

1. 打开命令提示符或终端窗口。
2. 键入以下命令：

```
aws configservice list-discovered-resources --resource-type
 MyCustomNamespace::Testing::WordPress
```

3. 按 Enter 键。

   您应该可以看到类似于如下所示的输出内容：

```
{
    "resourceIdentifiers": [
        {
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001"
        }
    ]
}
```

4. 键入以下命令：

```
aws configservice batch-get-resource-config --resource-keys '[ { "resourceType":
 "MyCustomNamespace::Testing::WordPress", "resourceId": "resource-001" } ]'
```

5. 按 Enter 键。

   您应该可以看到类似于如下所示的输出内容：

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
        {
            "configurationItemCaptureTime": 1569605832.673,
            "resourceType": "MyCustomNamespace::Testing::WordPress",
            "resourceId": "resource-001",
            "configurationStateId": "1569605832673",
            "awsRegion": "us-west-2",
            "version": "1.3",
            "supplementaryConfiguration": {},
            "configuration": "{\"Id\":\"resource-001\",\"Name\":\"My example custom
 resource.\",\"PublicAccess\":false}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "AccountId"
        }
    ]
}
```

删除第三方资源

您可以记录要删除的第三方资源或自定义资源类型的配置状态。

- 键入以下命令：

```
aws configservice delete-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-002
```

如果成功，则命令会执行，而没有附加输出。

使用 API 管理第三方资源类型的配置状态

您可以使用管理第三方资源或自定义资源类型的配置状态PutResourceConfig和DeleteResourceConfigAPI。有关详细信息，请参阅 API 参考。

- PutResourceConfig
- DeleteResourceConfig

区域支持

目前，以下区域中支持此功能：

区域名称	区域	Endpoint	协议
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS

区域名称	区域	Endpoint	协议
欧洲（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

标记您的 Amazon Config 资源

标签是为Amazon资源分配的标记。每个标签都包含您定义的一个键 和一个可选值。可以利用标签更轻松地管理、搜索和筛选资源。

标签可让您按各种标准 (例如用途、所有者或环境) 对 Amazon 资源进行分类。这在您拥有许多同类型资源时很有用 - 您可以根据分配给资源的标签快速识别特定资源。您可以将一个或多个标签分配给Amazon资源的费用。每个标签都有关联的值。

我们建议您针对每类资源设计一组标签，以满足您的需要。使用一组连续的标签键，管理时会更加轻松。Amazon资源的费用。您可以根据添加的标签搜索和筛选资源。

标签将会严格地作为字符串进行解析，并且不会自动分配至您的资源。您可以修改标签的密钥和值，还可以随时删除资源的标签。您可以将标签的值设为空的字符串，但是不能将其设为空值。如果您添加的标签的值与该实例上现有标签的值相同，新的值就会覆盖旧值。如果删除资源，资源的所有标签也会被删除。

可以使用 Amazon Command Line Interface（Amazon CLI）和 Amazon Config API 参考来处理标签。

与标记相关的限制

下面是适用于标签的基本限制。

限制	说明
每个资源的最大标签数	50
最大密钥长度	128 个 Unicode 字符（采用 UTF-8 格式）
最大值长度	256 个 Unicode 字符（采用 UTF-8 格式）
前缀限制	请勿在标签名称或值中使用 `aws:` 前缀，因为它专为 Amazon 使用预留。您无法编辑或删除带此前缀

限制	说明
	的标签名称或值。具有此前缀的标签不计入每个资源的标签数限制。
字符限制	标签只能包含 Unicode 字母、数字、空格或以下符号：_ . : / = + - @

使用 Amazon Config API 操作管理标签

基于标签的访问控制可用于三种资源：`ConfigurationAggregator`、`AggregationAuthorization` 和 `ConfigRule`。使用以下命令添加、更新、列出和删除资源标签。

- ListTagsForResource
- TagResource
- UntagResource

Amazon Config 发送到 Amazon SNS 主题的通知

可以配置 Amazon Config，将配置更改和通知流式传输到 Amazon SNS 主题。例如，更新资源时，可以通过电子邮件接收通知，查看更改。也可以在 Amazon Config 针对您的资源评估自定义规则或托管规则时收到通知。

Amazon Config 针对以下事件发送通知：

- 资源的配置项发生变更。
- 为您的账户传输了资源配置历史记录。
- 为您的账户启动并传输了已记录资源的配置快照。
- 您的资源的合规性状态以及它们是否符合您的规则。
- 针对您的资源开始评估规则。
- Amazon Config 未能向您的账户传输通知。

主题

示例配置项变更通知

Amazon Config使用 Amazon SNS 向订阅终端节点传送通知。这些通知可以提供配置快照和配置历史记录的传送状态，并提供 Amazon Config 在记录的 Amazon 资源的配置发生更改时创建的每个配置项。Amazon

Config 还会发送指示您的资源是否符合规则的通知。如果您选择通过电子邮件发送通知，则可在您的电子邮件客户端应用程序中，根据电子邮件的主题行和消息正文使用筛选条件。

以下是一个 Amazon SNS 通知示例负载，该通知在以下情况下生成：Amazon Config检测到 Amazon Elastic Block Store 卷`vol-ce676ccc`已附加到实例的 ID 为`i-344c463d`. 此通知包含针对资源的配置项变更。


```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "accountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
```

```
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/
Ro9QTmiTNcEjQ5kB8wGsRWVrk/whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kgapIo4CtC
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```


存在关系的资源的配置项

如果某个资源与其他资源关联，则更改该资源会导致产生多个配置项。以下示例显示了 Amazon Config 如何为存在关系的资源创建配置项。

1. 您有一个 ID 为的 Amazon EC2 实例`i-007d374c8912e3e90`，并且该实例与 Amazon EC2 安全组关联，`sg-c8b141b4`.
2. 您更新 EC2 实例，将安全组变更为另一安全组 `sg-3f1fef43`。
3. 由于 EC2 实例与另一资源关联，因此 Amazon Config 将创建多个配置项，如以下示例所示：

更换安全组时，此通知包含针对 EC2 实例的配置项变更。


```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
```

```
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Relationships.0": {
                    "previousValue": {
                        "resourceId": "sg-c8b141b4",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                },
                "Configuration.NetworkInterfaces.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-2",
                            "groupId": "sg-3f1fef43"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
```

```
                            "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
                                "publicIp": "54.175.43.43",
                                "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                                "ipOwnerId": "amazon"
                            }
                        }]
                    },
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
                    "name": "Is associated with SecurityGroup"
                },
                {
                    "resourceId": "subnet-2372be7b",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Subnet",
                    "name": "Is contained in Subnet"
```

```
        },
        {
            "resourceId": "vol-0a2d63a256bce35c5",
            "resourceName": null,
            "resourceType": "AWS::EC2::Volume",
            "name": "Is attached to Volume"
        },
        {
            "resourceId": "vpc-14400670",
            "resourceName": null,
            "resourceType": "AWS::EC2::VPC",
            "name": "Is contained in Vpc"
        }
    ],
    "configuration": {
        "instanceId": "i-007d374c8912e3e90",
        "imageId": "ami-9be6f38c",
        "state": {
            "code": 16,
            "name": "running"
        },
        "privateDnsName": "ip-172-31-16-84.ec2.internal",
        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
        "stateTransitionReason": "",
        "keyName": "ec2-micro",
        "amiLaunchIndex": 0,
        "productCodes": [],
        "instanceType": "t2.micro",
        "launchTime": "2017-01-09T20:13:28.000Z",
        "placement": {
            "availabilityZone": "us-east-2c",
            "groupName": "",
            "tenancy": "default",
            "hostId": null,
            "affinity": null
        },
        "kernelId": null,
        "ramdiskId": null,
        "platform": null,
        "monitoring": {"state": "disabled"},
        "subnetId": "subnet-2372be7b",
        "vpcId": "vpc-14400670",
        "privateIpAddress": "172.31.16.84",
        "publicIpAddress": "54.175.43.43",
        "stateReason": null,
        "architecture": "x86_64",
        "rootDeviceType": "ebs",
        "rootDeviceName": "/dev/xvda",
        "blockDeviceMappings": [{
            "deviceName": "/dev/xvda",
            "ebs": {
                "volumeId": "vol-0a2d63a256bce35c5",
                "status": "attached",
                "attachTime": "2017-01-09T19:36:03.000Z",
                "deleteOnTermination": true
            }
        }],
        "virtualizationType": "hvm",
        "instanceLifecycle": null,
        "spotInstanceRequestId": null,
        "clientToken": "bIYqA1483990561516",
        "tags": [{
            "key": "Name",
            "value": "value"
        }],
        "securityGroups": [{
```

```
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43"
            }],
            "sourceDestCheck": true,
            "hypervisor": "xen",
            "networkInterfaces": [{
                "networkInterfaceId": "eni-fde9493f",
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "description": "",
                "ownerId": "123456789012",
                "status": "in-use",
                "macAddress": "0e:36:a2:2d:c5:e0",
                "privateIpAddress": "172.31.16.84",
                "privateDnsName": "ip-172-31-16-84.ec2.internal",
                "sourceDestCheck": true,
                "groups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "attachment": {
                    "attachmentId": "eni-attach-85bd89d9",
                    "deviceIndex": 0,
                    "status": "attached",
                    "attachTime": "2017-01-09T19:36:02.000Z",
                    "deleteOnTermination": true
                },
                "association": {
                    "publicIp": "54.175.43.43",
                    "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                    "ipOwnerId": "amazon"
                },
                "privateIpAddresses": [{
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "primary": true,
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    }
                }]
            }],
            "iamInstanceProfile": null,
            "ebsOptimized": false,
            "sriovNetSupport": null,
            "enaSupport": true
        },
        "supplementaryConfiguration": {},
        "tags": {"Name": "value"},
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
        "configurationStateId": 1484002214328,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "i-007d374c8912e3e90",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
        "awsRegion": "us-east-2",
        "availabilityZone": "us-east-2c",
        "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
        "resourceCreationTime": "2017-01-09T20:13:28.000Z"
    },
    "notificationCreationTime": "2017-01-09T22:50:15.928Z",
    "messageType": "ConfigurationItemChangeNotification",
```

```
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

此通知包含针对与该实例关联的 EC2 安全组 `sg-3f1fef43` 的配置项变更。

```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
```

```
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVxNBQEi4k8
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


示例配置历史记录传输通知

配置历史记录是某一资源类型在一段时间内的配置项的集合。下面是 Amazon Config 在针对您的账户传输 CloudTrail 跟踪资源的配置历史记录时发送的示例通知。


```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for Account
 123456789012",
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-
east-2/2016/9/27/ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhrbCBgX5ma
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


示例配置快照传输开始通知

下面是 Amazon Config 在 Amazon Config 开始针对您的账户传输配置快照时发送的示例通知。


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
```

```
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for Account
 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm+H9wavcwXB9XECelHhRW70Y
+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

示例配置快照传输通知

配置快照是所有已记录资源的配置项及其在您账户中的配置的集合。下面是 Amazon Config 在针对您的账户传输配置快照时发送的示例通知。

```
{
    "Type": "Notification",
    "MessageId": "9fc82f4b-397e-5b69-8f55-7f2f86527100",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Completed for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "16da64e4-cb65-4846-b061-e6c3ba43cb96",
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigSnapshot/123456789012_Config_us-east-2_ConfigSnapshot_20160927T183939Z_16da64e4-
cb65-4846-b061-e6c3ba43cb96.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T18:39:39.853Z",
        "messageType": "ConfigurationSnapshotDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T18:39:40.062Z",
    "SignatureVersion": "1",
    "Signature": "PMkWfUuj/fKIEXA7s2wTDLbZoF/MDsUkPspYghOpwu9n6m+C
+zrm0cEZXPxxJPvhnWozG7SVqkHYf9QgI/diW2twP/HPDn5GQs2rNDc+YlaByEXnKVtHV1Gd4r1kN57E/
oOW5NVLNczk5ymxAW+WGdptZJkCgyVuhJ28s08m3Z3Kqz96PPSnXzYZoCfCn/
yP6CqXoN7olr4YCbYxYwn8zOUYcPmc45yYNSUTKZi+RJQRnDJkL2qb+s4h9w2fjbBBj8xe830VbFJqbHp7UkSfpc64Y
+tRvmMLY5CI1cYrnuPRhTLdUk+R0sshg5G+JMtSLVG/TvWbjz44CKXJprjIQg==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

示例合规性变更通知

当 Amazon Config 针对自定义规则或托管规则评估您的资源时，Amazon Config 会发送一个通知来指明资源是否符合该规则。

下面是当 CloudTrail 跟踪资源符合 `cloudtrail-enabled` 托管规则时的示例通知。


```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr15gdHozx8
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

示例规则评估开始通知

Amazon Config 在开始针对您的资源评估您的自定义规则或托管规则时会发送通知。下面是 Amazon Config 在开始评估 `iam-password-policy` 托管规则时的示例通知。


```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


示例过大配置项变更通知

当 Amazon Config 检测到资源的配置项变更时，会发送配置项通知。如果通知超过了 Amazon Simple Notification Service (Amazon SNS) 允许的最大大小，则通知会包含配置项的简短摘要。您可以在中指定的 Amazon S3 存储桶位置查看完整通知。`s3BucketLocation`字段中返回的子位置类型。

以下示例通知演示适用于 Amazon EC2 实例的配置项。通知中包含变更摘要以及通知在 Amazon S3 存储桶中的位置。


```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/resourceId_14b76876-7969-4097-ab8e-a31942b02e80?
time=2016-10-06T16:46:16.261Z

    The full configuration item change notification for this resource exceeded the maximum
 size allowed by Amazon Simple Notification Service (SNS). A summary of the configuration
 item is provided here. You can view the complete notification in the specified Amazon S3
 bucket location.

    New State Record Summary:
    ---------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
```

```
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/resourceId_14b76876-7969-4097-
ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "my-bucket/AWSLogs/123456789012/Config/
us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

示例传输失败通知

Amazon Config在以下情况下发送失败通知Amazon Config无法向 Amazon S3 存储桶传输配置快照或过大配置项更改通知。请确认您指定了有效的 Amazon S3 存储桶。

```
View the Timeline for this Resource in the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

     The full configuration item change notification for this resource exceeded the maximum
 size allowed by Amazon Simple Notification Service (SNS). A summary of the configuration
 item is provided here. You can view the complete notification in the specified Amazon S3
 bucket location.

    New State Record Summary:
    -----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
```

```
       "errorMessage": "Failed to deliver notification to bucket: bucket-example for
account 123456789012 in region us-west-2."
     },
     "notificationCreationTime": "2016-10-06T16:46:13.749Z",
     "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
     "recordVersion": "1.0"
   }
```

使用 Amazon Config 规则评估资源

使用 Amazon Config 评估您的 Amazon 资源的配置设置。您可以通过创建 Amazon Config 规则进行评估，这些规则代表您理想的配置设置。Amazon Config 提供可自定义的预定义规则（称作托管规则）来帮助您开始进行评估。在 Amazon Config 持续跟踪您的资源中出现的配置更改时，它会检查这些更改是否违反了规则中的任何条件。如果某个资源违反了规则，则 Amazon Config 会将该资源和规则标记为不合规。

例如，当创建 EC2 卷时，Amazon Config 可以按照需要卷加密的规则来评估该卷。如果卷没有加密，Amazon Config 会将卷和规则标记为不合规。Amazon Config 还可以在您的所有资源中检查有无账户范围内的要求。例如，Amazon Config 可以检查账户中的 EC2 卷数是否在所需总数内，或者账户是否使用 Amazon CloudTrail 进行日志记录。

服务相关规则是支持其他规则的唯一类型的托管规则Amazon要创建的服务Amazon Config账户中的规则。这些规则已预定义以包含调用其他所需的所有权限Amazon服务代表您。这些规则类似于标准Amazon在你的服务中推荐Amazon用于合规性验证。有关更多信息，请参阅 服务相关联Amazon ConfigRule (p. 235)。

Amazon Config 控制台将显示您的规则与资源的合规性状态。您可以查看您的 Amazon 资源在整体上对所需配置的符合情况，并了解哪些特定资源不合规。您也可以使用 Amazon CLI、Amazon Config API 和 Amazon 开发工具包来请求 Amazon Config 服务，以获取合规性信息。

通过使用 Amazon Config 评估您的资源配置，您可以评估资源配置对内部实践、行业指南和法规的遵循情况。

对于支持的区域Amazon Config规则，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.

您最多可以创建 400 个Amazon Config账户中每个区域的规则。有关更多信息，请参阅 Amazon Config 限制。

您还可以创建自定义规则来评估 Amazon Config 未记录的其他资源。有关更多信息，请参阅 评估其他资源类型 (p. 191)。

主题

区域支持

目前，Amazon Config以下区域支持规则：

区域名称	区域	Endpoint	协议
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Amazon GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
Amazon GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧洲（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧洲（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

区域名称	区域	Endpoint	协议
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

部署Amazon Config跨越成员账户的规则Amazon以下区域支持组织。

区域名称	区域	Endpoint	协议
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

区域名称	区域	Endpoint	协议
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

的组成部分Amazon ConfigRule

Amazon Config规则评估您的配置设置Amazon资源的费用。有两种类型的规则：Amazon Config托管规则和Amazon Config自定义规则。托管规则是由以下人员创建的预定义、可自定义的规则Amazon Config. 有关托管规则的列表，请参阅。的列表Amazon Config托管规则.

自定义规则是您可以使用 Guard 或Amazon Lambda函数。Guard (警卫 GitHubRepository) 是一个 policy-as-code 允许您编写由强制执行的策略的语言Amazon Config自定义策略规则。Amazon Lambda使用您上传的自定义代码来评估自定义规则。它由事件源发布给它的事件调用，其中Amazon Config在自定义规则启动时调用。

本页讨论规则定义的结构以及有关如何使用 Python 编写规则的最佳实践Amazon Config规则开发工具包 (RDK) 和Amazon Config规则开发工具包库 (RDKlib)。有关演示如何创建的演练Amazon Config自定义策略规则，请参阅创建Amazon Config自定义策略规则. 有关演示如何创建的演练Amazon Config自定义 Lambda 规则，请参阅创建Amazon Config自定义 Lambda 规则.

目录

规则定义

Amazon Config规则定义包含以下字段：

- 标识符
- 默认名称
- description
- 范围
- SourceTails
- compulsoryInputParameter详细信息
- optionalInputParameter详细信息
- 标签

下面的 JSON 示例介绍了规则定义代码部署-ec2-minimum-healthy-hosts-configured托管规则。

```
{
  "identifier": "CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED",
  "defaultName": "codedeploy-ec2-minimum-healthy-hosts-configured",
  "description": "Checks if the deployment group for EC2/On-Premises Compute Platform
 is configured with a minimum healthy hosts fleet percentage or host count greater
 than or equal to the input threshold. The rule is NON_COMPLIANT if either is below the
 threshold.",
  "scope": {
    "resourceTypes": [
      "AWS::CodeDeploy::DeploymentGroup"
    ]
  },
  "sourceDetails": [
    {
      "eventSource": "AWS_CONFIG",
      "messageType": "ConfigurationItemChangeNotification"
    },
    {
      "eventSource": "AWS_CONFIG",
      "messageType": "OversizedConfigurationItemChangeNotification"
    }
  ],
  "compulsoryInputParameterDetails": {},
  "optionalInputParameterDetails": {
    "minimumHealthyHostsFleetPercent": {
      "type": "int",
      "description": "Minimum percentage of healthy hosts fleet during deployment. Default
 value is set to 66 percent.",
      "defaultValue": "66"
    },
    "minimumHealthyHostsHostCount": {
      "type": "int",
      "description": "Minimum number of healthy hosts in fleet during deployment. Default
 value is set to 1.",
      "defaultValue": "1"
    }
  },
  "labels": [
    "CodeDeploy"
  ]
}
```

规则元数据

标识符

规则标识符用作Amazon Config托管规则。规则标识符是用下划线写入的。例如，`CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED`是规则标识符和`codedeploy-ec2-minimum-healthy-hosts-configured`是规则名称。规则标识符用于在以下情况下标识规则创建Amazon Config托管规则使用Amazon CloudFormation模板或者在调用PutConfigRuleAPI。

> **Note**
>
> 对于某些规则，规则标识符与规则名称不同。例如，规则标识符`restricted-ssh`是`INCOMING_SSH_DISABLED`.

默认名称

默认名称是规则实例在默认情况下将获得的名称。

description

规则描述为规则评估的内容提供了上下文。这些区域有：Amazon Config控制台具有 256 个字符的限制。作为最佳实践，规则描述应带有 “检查是否”，并包括对不合规情形的描述。服务名称应以完整开

头写成Amazon或在规则描述中首次提及亚马逊。例如，Amazon CloudTrail或 Amazon CloudWatch INSTEAD CloudTrail 要么 CloudWatch 首次使用。服务名称可以在后续引用后缩写。

范围

作用域决定了规则所针对的资源类型。如果规则是更改触发的，或者规则既是更改触发的又是周期性的，则该选项是必需的；对于周期性规则，此选项是可选的。有关支持的资源类型的列表，请参阅支持的资源类型。

SourceTails

SourceDetails 决定了规则的触发器类型。`ConfigurationItemChangeNotification`和`OversizedConfigurationItemChangeNotification`用于更改触发的规则。当 Amazon Config 检测到资源的配置项变更时，会发送配置项通知。如果通知超过了 Amazon 简单通知服务 (Amazon SNS) 允许的最大大小，则通知会包含配置项的简短摘要。您可以在 s3 中指定的 S3 存储桶位置查看完整通知BucketLocation 字段中返回的子位置类型。

`ScheduleNotification`用于周期性规则。如果规则定期评估并通过配置更改进行评估，则可以使用所有三种类型的通知。有关更多信息，请参阅 。为指定触发器Amazon ConfigRule

compulsoryInputParameter详细信息

这些区域有： compulsoryInputParameter详细信息用于规则进行评估所需的参数。例如，`access-keys-rotated`托管规则包括`maxAccessKeyAge`作为必需的参数。如果需要参数，则不会将其标记为（可选）。必须为每个参数指定一个类型。类型可以是“字符串”、“int”、“double”、“CSV”、“布尔”和”StringMap“。

optionalInputParameter详细信息

这些区域有： optionalInputParameter详细信息用于规则进行评估的可选参数。例如，`codedeploy-ec2-minimum-healthy-hosts-configured`托管规则包括`minimumHealthyHostsFleetPercent`和`minimumHealthyHostsHostCount`作为可选参数。必须为每个参数指定一个类型。类型可以是“字符串”、“int”、“double”、“CSV”、“布尔” 和”StringMap“。

标签

标签可用于标记规则。例如，`codedeploy-auto-rollback-monitor-enabled`、`codedeploy-ec2-minimum-healthy-hosts-configured`, 和`codedeploy-lambda-allatonce-traffic-shift-disabled`托管规则都包含标签`CodeDeploy`.

规则结构

本部分包含了有关使用Amazon Config规则开发工具包 (RDK) 和Amazon Config规则开发工具包库 (RDKlib)。有关 RDK 或 RDKLib 的更多信息，请参阅。aws-config-rdk 和aws-config-rdklib GitHub 存储库。

写规则

先决条件

1. 按中的步骤操作。安装Amazon CLI.
2. 按中的步骤操作。设置Amazon Config使用控制台要么设置Amazon Config用Amazon CLI. 有关的信息Amazon所在的区域Amazon Config受支持，请从Amazon区域服务列表.
3. 使用 pip 的推荐方法安装 RDK：

```
pip install rdk
```

Note

在使用 pip 之前，请确保它已安装在您的机器上。

4. 使用 pip 的推荐方法安装 RDKLib：

```
pip install rdklib
```

Note

在使用 pip 之前，请确保它已安装在您的机器上。

更改触发的规则

1. 要创建由指定资源类型更改触发的规则，请运行以下命令：

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-types AWS::Resource::Type
```

以下示例创建由更改触发的规则`AWS::IAM::User`资源类型：

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User
```

以下是可以与`rdk create`更改触发规则的命令：

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a rule
 to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

Note

要使用 RDKLib，必须将规则的运行时设置为`python3.6-lib`.

跑完之后`rdk create`，您应该会看到一个新目录，其中包含规则名称和 3 个文件：

- *RULE_NAME*.py-存储规则逻辑的 Python 文件
- *RULE_NAME*_test.py-存储规则单元测试的 Python 文件
- parameters.json-用于 RDK 部署设置的 JSON 文件

2. 下一个步骤是编写规则逻辑。你只需要编辑*RULE_NAME*.py 文件。如果你打开*RULE_NAME*.py 文件，您将看到一个模板，您可以在其中添加规则逻辑。以下是为 MFA_ENABLED_RULE 生成的模板：

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ################################
        # Add your custom logic here. #
        ################################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
```

```
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

以下示例是带有规则逻辑的 MFA_ENABLED_RULE 模板的编辑版本。规则检查 IAM 用户是否启用了多重身份验证 (MFA)。如果 IAM 用户未启用 MFA，则规则为 NON_COMPLIANT。有关模板中提供的规则逻辑和方法的更多信息，请参阅规则逻辑 (p. 118).

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):

        username = configuration_item.get("resourceName")

        iam_client = client_factory.build_client("iam")

        response = iam_client.list_mfa_devices(UserName=username)

        # Scenario:1 IAM user has MFA enabled.
        if response["MFADevices"]:
            return [Evaluation(ComplianceType.COMPLIANT)]

        # Scenario:2 IAM user has MFA not enabled.
        annotation = "MFA needs to be enabled for user."
        return [Evaluation(ComplianceType.NON_COMPLIANT, annotation=annotation)]

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. 下一个步骤是在 RDKLib 层中安装 RDKLib 层。Amazon要么使用Amazon控制台或Amazon CLI. RDKlib的设计用作Amazon Lambda层。它允许您使用库，而无需将其包含在部署软件包中。

   - 使用以下命令安装 RDKLib 层Amazon控制台，请执行以下步骤：

     1. 打开 Amazon Lambda 控制台，地址：https://console.aws.amazon.com/lambda/。
     2. Select创建函数.
     3. 在存储库的创建函数页面，选择浏览无服务器应用程序存储库，然后在搜索框中，输入rdklib.
     4. 查看函数详情，然后进行部署。您不必进行任何更改。
     5. 在左侧导航窗格中，依次选择相应的层页. 然后选择您刚刚创建的 Lambda 层，然后复制 Lambda 层的 Amazon 资源名称 (ARN)。在部署规则时，您将需要 Lambda 层的 ARN。

   - 使用以下命令安装 RDKLib 层Amazon CLI，运行以下命令：

1. 为 rdklib-layer 创建更改集。

```
aws serverlessrepo create-cloud-formation-change-set --application-id
 arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --stack-
name RDKlib-Layer
```

它将返回以下输出：

```
{
    "ApplicationId": "arn:aws:serverlessrepo:ap-
southeast-1:711761543063:applications/rdklib",
    "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
    "SemanticVersion": "0.1.0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/serverlessrepo-
RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
}
```

2. 执行变更集。您可以复制/粘贴完整的变更集 ARN (ChangeSetId 来自上一步生成的输出），以自定义以下命令：

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. 返回作为已部署堆栈一部分的所有关联资源。

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

它将返回以下输出：

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. 从上一步中生成的输出中复制 Lambda 层的 ARN。Lambda 层的 ARN 是`PhysicalResourceId`.

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-layer:1"
```

4. 下一步是为 Lambda 函数提供一个要担任的角色。默认情况下，Lambda 函数会尝试假设`AWSServiceRoleForConfig`角色，这是不允许的。您需要使用创建角色`AWS_ConfigRole`托管策略。该角色必须与具有信任关系Amazon Config并且 /rdk/ 路径下的所有角色都应代入该角色。以下是示例信任策略：

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

使用此信任策略，运行以下命令：

```
aws iam create-role --role-name your-role-name --assume-role-policy-document file://
trust-policy.json
```

现在，运行以下命令来更新的输入参数ExecutionRoleName并提供角色名称：

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-name"}'
```

您还可以使用rdk modify使用以下标志更新更改触发的规则详细信息：

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a rule
 to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
```

5. 最终步骤是部署规则。要部署规则，请使用步骤 3 中的 Lambda 层的 ARN 运行以下命令：

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. 该规则现已部署。您可以使用Amazon Config控制台检查规则是否正按预期工作。

定期规则

1. 要创建针对指定资源类型定期触发的规则，请运行以下命令：

```
rdk create YOUR_RULE_NAME --runtime python3.6-lib --resource-types AWS::Resource::Type
 --maximum-frequency EXECUTION_FREQUENCY
```

以下示例创建一个规则，此规则每 24 小时为AWS::IAM::User资源类型：

```
rdk create MFA_ENABLED_RULE --runtime python3.6-lib --resource-types AWS::IAM::User --
maximum-frequency TwentyFour_Hours
```

以下是可以与`rdk create`定期规则的命令:

```
rdk create RULE_NAME
    --runtime pythonX.X-lib // Python runtime version
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a rule
 to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on a
 periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

> **Note**
>
> 要使用 RDKLib，必须将规则的运行时设置为`python3.6-lib`.

跑完之后`rdk create`，您应该会看到一个新目录，其中包含规则名称和 3 个文件：

- *RULE_NAME*.py-存储规则逻辑的 Python 文件
- *RULE_NAME*_test.py-存储规则单元测试的 Python 文件
- parameters.json-用于 RDK 部署设置的 JSON 文件

2. 下一个步骤是编写规则逻辑。你只需要编辑*RULE_NAME*.py 文件。如果你打开*RULE_NAME*.py 文件，您将看到一个模板，您可以在其中添加规则逻辑。以下是为 MFA_ENABLED_RULE 生成的模板：

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType

APPLICABLE_RESOURCES = ['AWS::IAM::User']

class MFA_ENABLED_RULE(ConfigRule):

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ################################
        # Add your custom logic here. #
        ################################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

    #def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
    #    pass

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

模板默认为更改触发的规则。相反，将你的逻辑添加到`evaluate_periodic`方法。以下示例是带有规则逻辑的 MFA_ENABLED_RULE 模板的编辑版本。规则检查 IAM 用户是否启用了多重身份验证

(MFA)。如果 IAM 用户未启用 MFA，则规则为 NON_COMPLIANT。有关模板中提供的规则逻辑和方法的更多信息，请参阅规则逻辑 (p. 118).

```
from rdklib import ComplianceType, ConfigRule, Evaluation, Evaluator

APPLICABLE_RESOURCES = ["AWS::IAM::User"]

class MFA_ENABLED_RULE(ConfigRule):l

    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        evaluations = []

        iam_client = client_factory.build_client("iam")

        paginator = iam_client.get_paginator("list_users")
        response_iterator = paginator.paginate()

        for response in response_iterator:
            for user in response["Users"]:
                username = user["UserName"]
                response = iam_client.list_mfa_devices(UserName=username)

                # Scenario:1 IAM user has MFA enabled.
                if response["MFADevices"]:
                    evaluations.append(Evaluation(ComplianceType.COMPLIANT, username,
 "AWS::IAM::User"))

                # Scenario:2 IAM user has MFA not enabled.
                if not response["MFADevices"]:
                    annotation = "MFA needs to be enabled for user."
                    evaluations.append(
                        Evaluation(ComplianceType.NON_COMPLIANT, username,
 "AWS::IAM::User", annotation=annotation)
                    )
        return evaluations

    def evaluate_parameters(self, rule_parameters):
        valid_rule_parameters = rule_parameters
        return valid_rule_parameters

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = MFA_ENABLED_RULE()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

3. 下一个步骤是在 RDKLib 层中安装 RDKLib 层。Amazon要么使用Amazon控制台或Amazon CLI. RDKlib的设计用作Amazon Lambda层。它允许您使用库，而无需将其包含在部署软件包中。

   - 使用以下命令安装 RDKLib 层Amazon控制台，请执行以下步骤：

     1. 打开 Amazon Lambda 控制台，地址：https://console.aws.amazon.com/lambda/。
     2. Select创建函数.
     3. 在存储库的创建函数页面，选择浏览无服务器应用程序存储库，然后在搜索框中，输入rdklib.
     4. 查看函数详情，然后进行部署。您不必进行任何更改。
     5. 在左侧导航窗格中，依次选择相应的层页. 然后选择您刚刚创建的 Lambda 层，然后复制 Lambda 层的 Amazon 资源名称 (ARN)。在部署规则时，您将需要 Lambda 层的 ARN。

   - 使用以下命令安装 RDKLib 层Amazon CLI，运行以下命令：

     1. 为 rdklib-layer 创建更改集。

```
aws serverlessrepo create-cloud-formation-change-set --application-id
 arn:aws:serverlessrepo:ap-southeast-1:711761543063:applications/rdklib --stack-
name RDKlib-Layer
```

它将返回以下输出：

```
{
    "ApplicationId": "arn:aws:serverlessrepo:ap-
southeast-1:711761543063:applications/rdklib",
    "ChangeSetId": "arn:aws:cloudformation:us-east-1:123456789012:changeSet/
a3d536322-585e-4ffd-9e2f-552c8b887d6f/ffe7ff5c-ab38-4ab9-b746-9c1617ca95c1",
    "SemanticVersion": "0.1.0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/serverlessrepo-
RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53"
}
```

2. 执行变更集。您可以复制/粘贴完整的变更集 ARN (ChangeSetId 来自上一步生成的输出），以自定义以下命令：

```
aws cloudformation execute-change-set --change-set-name NAME_OF_THE_CHANGE_SET
```

3. 返回作为已部署堆栈一部分的所有关联资源。

```
aws cloudformation describe-stack-resources --stack-name serverlessrepo-RDKlib-
Layer
```

它将返回以下输出：

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

4. 从上一步中生成的输出中复制 Lambda 层的 ARN。Lambda 层的 ARN 是`PhysicalResourceId`.

```
"PhysicalResourceId": "arn:aws:lambda:us-east-1:123456789012:layer:rdklib-layer:1"
```

4. 下一步是为 Lambda 函数提供一个要担任的角色。默认情况下，Lambda 函数会尝试假设`AWSServiceRoleForConfig`角色，这是不允许的。您需要使用创建角色`AWS_ConfigRole`托管策略。该角色必须与具有信任关系Amazon Config并且 /rdk/ 路径下的所有角色都应代入该角色。以下是示例信任策略：

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-ID:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": "arn:aws:iam::account-ID:role/rdk/*"
        }
      }
    }
  ]
}
```

使用此信任策略，运行以下命令：

```
aws iam create-role --role-name your-role-name --assume-role-policy-document file://
trust-policy.json
```

现在，运行以下命令来更新的输入参数ExecutionRoleName并提供角色名称：

```
rdk modify YOUR_RULE_NAME --input-parameters '{"ExecutionRoleName":"your-role-name"}'
```

您还可以使用rdk modify使用以下标志更新定期规则详细信息：

```
rdk modify RULE_NAME
    --input-parameters REQUIRED_PARAMETERS // Parameters that are required for a rule
 to do its evaluation
    --optional-parameters OPTIONAL_PARAMETERS // Parameters that are optional for a
 rule to do its evaluation
    --resource-types AWS::Resource::Type // Resource type(s) that the rule targets
    --maximum-frequency EXECUTION_FREQUENCY // How often the rule should be run on a
 periodic trigger.
 One of ['One_Hour','Three_Hours','Six_Hours','Twelve_Hours','TwentyFour_Hours']
```

5. 最终步骤是部署规则。要部署规则，请使用步骤 3 中的 Lambda 层的 ARN 运行以下命令：

```
rdk deploy YOUR_RULE_NAME --rdklib-layer-arn YOUR_RDKLIB_LAYER_ARN
```

6. 该规则现已部署。您可以使用Amazon Config控制台检查规则是否正按预期工作。

规则逻辑

以下 Python 代码示例是使用 RDK 和 RKDLib 编写规则的模板。你应该只在evaluate_parameters、evaluate_change, 和evaluate_periodic方法，或者在需要时编写全新的函数来帮助逻辑。有关使用 RDK 和 RDKlib 编写规则的先决条件，请参阅先决条件 (p. 110).

```
from rdklib import Evaluator, Evaluation, ConfigRule, ComplianceType
```

```
APPLICABLE_RESOURCES = ["AWS::Resource::Type"]

# When you create a rule, the class name will be the name you give the rule when you create
 it instead of ConfigRule
class ConfigRule (ConfigRule):

    def evaluate_parameters(self, rule_parameters):
        return rule_parameters

    def evaluate_change(self, event, client_factory, configuration_item,
 valid_rule_parameters):
        ################################
        # Add your custom logic here. #
        ################################

    def evaluate_periodic(self, event, client_factory, valid_rule_parameters):
        ################################
        # Add your custom logic here. #
        ################################

################################
# DO NOT MODIFY ANYTHING BELOW #
################################
def lambda_handler(event, context):
    my_rule = ConfigRule()
    evaluator = Evaluator(my_rule, APPLICABLE_RESOURCES)
    return evaluator.handle(event, context)
```

适用资源

APPLICABLE_RESOURCES是规则所针对的资源类型。如果使用，则该变量应为设置为规则所针对的资源类型的全局变量。有关支持的资源类型的列表，请参阅支持的资源类型。

评估参数

描述

此方法用于检查规则的输入参数是否有效。以下是最佳实践：

- 检查列出的参数数是否正确。
- 检查参数名称是否正确。
- 检查参数值的类型是否正确。
- 如果参数是整数，请检查参数是否在合理的范围之间。
- 如果参数具有有限数量的可能选项，请检查该参数是否为这些选项之一。
- 如果参数是字符串，请检查其长度是否合理，并修剪值前后的任何空格。
- 检查是否正确处理了区分大小写的问题。
- 尽可能限制参数输入。例如，如果您收到的是逗号分隔的 ARN 列表，请确保只允许使用逗号和 ARN 支持的字符。

参数

rule_parameters是规则的输入参数的字典。

返回语法

如果其中一个参数无效，则可以引发InvalidParametersErrorError:

```
from rdklib import InvalidParametersError
raise InvalidParametersError("Error message to display")
```

如果参数全部有效，则该方法应返回一个字典：

```
return valid_rule_parameters
```

评估_change

描述

此方法用于评估更改触发规则的逻辑。

参数

`event`是Amazon Lambda事件提供者Amazon Config. 它是 JSON 格式的文档，其中包含要运行的 Lambda 函数的数据。有关示例，请参阅。的示例事件Amazon ConfigRule.

`client_factory`是 ClientFactory 要用于规则的对象。这些区域有： ClientFactory 类创建或重用一个 boto3 客户端，它提供了一个低级接口Amazon服务。boto3 客户端方法映射为Amazon服务 API，这意味着服务操作将映射到同名的客户端方法，并提供对相同操作参数的访问权。有关可用服务的列表，请参阅。可用的服务在 Boto3 文档文档中。

的请求语法`client_factory`如下所示：

```
response = client_factory.build_client(
    service='string')
```

例如：

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> 的 boto3 名称Amazon服务是必需的。

`configuration_item`是完整配置 Item 的字典，即使过大。配置项代表一个 point-in-time 支持的各种属性的视图Amazon资源。有关内容的信息`ConfigurationItem`，请参阅ConfigurationItem中的 Amazon ConfigAPI 参考。

`valid_rule_parameters`是的输出`evaluate_parameters()`方法。

返回语法

该方法应返回以下一个或多个：

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

对于所有不合规的评估，您都应使用注释。例如：

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why the
 rule is NON_COMPLIANT")]]
```

评估_定期

描述

此方法用于评估周期性规则。

参数

`event`是Amazon Lambda事件提供者Amazon Config. 它是 JSON 格式的文档，其中包含要运行的 Lambda 函数的数据。有关示例，请参阅。的示例事件Amazon ConfigRule.

`client_factory`是 ClientFactory 要用于规则的对象。这些区域有： ClientFactory 类创建或重用一个 boto3 客户端，它提供了一个低级接口Amazon服务。boto3 客户端方法映射为Amazon服务 API，这意味着服务操作将映射到同名的客户端方法，并提供对相同操作参数的访问权。有关可用服务的列表，请参阅。可用的服务在 Boto3 文档文档中。

的请求语法`client_factory`如下所示：

```
response = client_factory.build_client(
    service='string')
```

例如：

```
iam_client = client_factory.build_client("iam")
```

> **Note**
>
> 的 boto3 名称Amazon服务是必需的。

`valid_rule_parameters`是的输出`evaluate_parameters()`方法。

返回语法

该方法应返回以下一个或多个：

```
[Evaluation(ComplianceType.COMPLIANT)]
```

```
[Evaluation(ComplianceType.NON_COMPLIANT)]
```

```
[Evaluation(ComplianceType.NOT_APPLICABLE)]
```

对于所有不合规的评估，您都应使用注释。例如：

```
[return [Evaluation(ComplianceType.NON_COMPLIANT, annotation="Explanation for why the
 rule is NON_COMPLIANT")]]
```

lambda_andler

描述

您应该不需要修改此方法。lambda 处理程序用于处理事件。该函数在以下时间运行Amazon Lambda传递`event`反对`handler`方法。有关更多信息，请参阅 Python 中的 Lambda 函数处理程序中的。

参数

`event`是Amazon Lambda事件提供者Amazon Config. 它是 JSON 格式的文档，其中包含要运行的 Lambda 函数的数据。有关示例，请参阅。的示例事件Amazon ConfigRule.

`context`是在运行时由 Lambda 将对象传递给函数。此对象提供的方法和属性包含此函数在运行时可以使用的信息和方法。请注意，在较新版本的 Lambda 中，不再使用上下文。

为 Amazon Config 规则指定触发器

在向账户中添加规则时，您可以指定希望 Amazon Config 何时运行此规则；这称作触发器。当触发器触发时，Amazon Config 对照规则评估您的资源配置。

目录

触发器类型

触发器有两种类型：

配置更改

当创建、更改或删除特定类型的资源时，Amazon Config 会针对规则运行评估。

通过定义规则的范围来选择哪些资源触发评估。范围可以包括：

- 一个或多个资源类型
- 资源类型和资源 ID 的组合
- 标签键和值的组合
- 当创建、更新或删除任何记录的资源时

Amazon Config 在检测到与规则的范围匹配的资源发生更改时运行评估。您可以使用范围来限制哪些资源触发评估。否则，当任何已记录的资源出现更改时，都会触发评估。

定期

Amazon Config 按照您选择的频率运行规则的评估（例如，每 24 小时）。

如果您选择配置更改和定期，Amazon Config当检测到配置更改时，以及按照您指定的频率调用您的 Lambda 函数。

具有触发器的规则示例

具有配置更改触发器的规则示例

1. 你添加Amazon Config托管规则，`S3_BUCKET_LOGGING_ENABLED`以检查 Amazon S3 存储桶是否启用了日志记录。
2. 规则的触发器类型是配置更改。Amazon Config当创建、更改或删除 Amazon S3 存储桶时，将针对规则运行评估。
3. 当存储桶更新时，配置更改触发此规则，Amazon Config 评估存储桶是否符合此规则。

具有定期触发器的示例规则

1. 向账户添加 Amazon Config 托管规则 `IAM_PASSWORD_POLICY`。此规则检查您的 IAM 用户的密码策略是否遵守您的账户策略，如最小长度或特定字符要求。
2. 此规则的触发器类型为定期。Amazon Config 将按您指定的频率（如每 24 小时）针对规则运行评估。
3. 每 24 小时都会触发该规则，Amazon Config评估您的 IAM 用户的密码是否符合规则。

具有配置更改和定期触发器的示例规则

1. 您创建一条自定义规则以评估是否 CloudTrail 您的账户中的跟踪已启用并针对所有区域开启了日志记录。
2. 您希望每当有跟踪创建、更新或删除时 Amazon Config 都运行规则评估。您还希望 Amazon Config 每 12 小时运行一次规则。
3. 对于触发器类型，选择配置更改和定期。

关闭配置记录器时的规则评估

如果您关闭配置记录器，Amazon Config 将停止记录对您资源配置的更改。这会在以下方面影响到您的规则评估：

- 具有定期触发器的规则将按照指定的频率持续运行评估。
- 具有配置更改触发器的规则不运行评估。
- 具有两种触发器类型的规则仅按照指定的频率运行评估。规则不为配置更改运行评估。
- 如果您针对具有配置更改触发器的规则运行按需评估，则规则将评估资源的最后已知状态，这是最后一个记录的配置项目。

Amazon Config 托管规则

Amazon Config 提供了 Amazon 托管规则（可自定义的预定义规则），Amazon Config 使用这些规则来评估您的 Amazon 资源是否符合常见的最佳实践。例如，您可以使用一个托管规则来快速开始评估是否特定标签会应用于您的资源。您可以设置和激活这些规则而无需通过编写代码来创建 Amazon Lambda 函数，如果您想要创建自定义规则这就是必需的。Amazon Config 控制台可以引导您完成托管规则的配置和激活过程。您还可以使用 Amazon Command Line Interface 或 Amazon Config API 来传递用于定义托管规则配置的 JSON 代码。

您可以自定义托管规则的行为以满足您的需求。例如，您可以定义规则的范围以便限定触发规则评估的资源，例如 EC2 实例或卷。您可以自定义规则的参数，以便定义您的资源为符合规则而必须具备的属性。例如，您可以自定义一个参数，以指定您的安全组应阻止传输到特定端口号的传入流量。

激活一项规则后，Amazon Config 会将您的资源与规则中的条件进行比较。完成这一初始评估后，Amazon Config 会在每次触发评估时继续执行评估。规则中会定义评估触发器，可以包括以下类型：

- 配置更改–Amazon Config配置更改当与规则范围匹配的任何资源的配置更改时，将触发评估。在 Amazon Config 发送配置项更改通知后，评估便会运行。
- 定期–Amazon Config按照您选择的频率运行规则的评估（例如，每 24 小时）。

Amazon Config 控制台可以显示哪些资源符合规则以及所遵循的规则。有关更多信息，请参阅 查看配置合规性 (p. 63)。

主题

Amazon Config 托管规则的列表

Amazon Config当前支持以下托管规则。

Note

为托管规则指定的默认值仅在使用Amazon控制台。不为 API、CLI 或开发工具包提供默认值。

主题

access-keys-rotated

检查活动访问密钥是否在中指定的天数内轮换`maxAccessKeyAge`. 如果访问密钥未轮换`maxAccessKeyAge` 天以上，则规则为 NON_COMPLIANT。

Note

此规则要求您在常规设置中启用 “包括全局资源”，以便对资源进行评估。
在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。

标识符：ACCESS_KEYS_ROTATED

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

maxAccessKeyAGE, 类型：int, 默认值：90

不轮换的最大天数。默认值为 90。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

alb-http-drop-invalid-已启用标头

检查规则是否评估Amazon应用程序负载均衡器 (ALB)，以确保将其配置为丢弃 http 标头。如果 routing.htp.drop_header_header_header_header_header_header_header_header_

标识符：ALB_HTTP_DROP_INVALID_HEADER_ENABLED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、欧洲（米兰）、欧洲（米兰）、非洲（开普敦）区域除外

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

alb-http-to-https-重定向检查

检查是否在应用程序负载均衡器的所有 HTTP 侦听器上都配置了 HTTP 到 HTTPS 重定向。如果 Application Load Balancer 的一个或多个 HTTP 侦听器未配置 HTTP 到 HTTPS 重定向，则规则为 NON_COMPLIANT。如果一个或多个 HTTP 侦听器转发到 HTTP 侦听器而不是重定向，则该规则也是不合规的。

标识符：ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）和非洲（开普敦）区域除外

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

api-gw-cache-enabled和加密

检查 Amazon API Gateway 阶段中的所有方法是否已启用并加密缓存。如果 Amazon API Gateway 阶段中的任何方法均未配置为缓存或者缓存未加密，则规则为 NON_COMPLIANT。

标识符：API_GW_CACHE_ENABLED_AND_ENABLED_ENCRYPTED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（开普敦）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

api-gw-endpoint-type-Check

检查 Amazon API 网关 API 是否属于规则参数中指定的类型`endpointConfigurationType`. 如果 REST API 与规则参数中配置的终端节点类型不匹配，则规则返回 NON_COMPLIANT。

标识符：API_GW_ENDPOINT_TYPE_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域以外的区域

参数：

endpointConfigurationTypes, 类型: 字符串

允许的逗号分隔列表 endpointConfigurationTypes. 允许的值包括 REGIONAL、PRIVATE 和 EDGE。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

api-gw-execution-logging-已启用

检查 Amazon API Gateway 阶段中的所有方法是否已启用日志记录。如果未启用日志记录，则该规则为 NON_COMPLIANT。如果是，则规则为 NON_COMPLIAN`loggingLevel`既不是 ERROR 也不是 INFO。

标识符: API_GW_EXECUTION_LOGGING_ENABLED

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）和非洲（开普敦）区域以外的区域

参数：

loggingLevel（可选），类型: 字符串, 默认值：错误，信息

用逗号分隔的特定日志记录级别的列表（例如，ERROR、INFO 或 ERROR, INFO）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

approved-amis-by-id

检查运行的实例是否使用了指定的 AMI。指定批准的 AMI ID 的列表。其 AMI 不在此列表中的正在运行的实例为 NON_COMPLIANT。

标识符：APPROVED_AMIS_BY_ID

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

amiIds, 类型: CSV

AMI ID (逗号分隔的列表，最多包含 10 个)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

approved-amis-by-tag

检查运行的实例是否使用了指定的 AMI。指定标识 AMI 的标签。其 AMI 未包含至少一个指定标签的正在运行的实例为 NON_COMPLIANT。

标识符: APPROVED_AMIS_BY_TAG

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

amisByTagKeyAndValue, 类型： StringMap, 默认：tag-key: tag-value，other-tag-key

按标签指定 AMI (逗号分隔的列表，最多包含 10 个；例如`tag-key:tag-value`; 即`tag-key1`将 AMI 与`tag-key1`、`tag-key2:value2`匹配`tag-key2`有值 2)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

autoscaling-group-elb-healthcheck-必需

检查与负载均衡器关联的 Auto Scaling ger typtyptyptyptyptElastic Load Balancing ptypt

标识符: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

autoscaling-launch-config-public-ip-已禁用

检查 Amazon EC2 Auto Scaling 组是否通过启动配置启用了公有 IP 地址。如果 Auto Scaling 组的启动配置为 NON_COMPLIANT AssociatePublicIpAddress 设置为 “真”。

标识符：AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud (US-East)、Amazon GovCloud (US-West)、亚太地区（雅加达）、亚太地区（大阪）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloudtrail-s3-dataevents-enabled

检查是否至少有一个Amazon CloudTrail 跟踪记录了所有 S3 存储桶的 Amazon S3 数据事件。如果未配置跟踪 S3 存储桶数据事件，则规则为 NON_COMPLIANT。

标识符: CLOUDTRAIL_S3_DATAEVENTS_已启用

触发器类型: 定期

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域以外的区域

参数：

S3BucketNames （ 可选 ）, 类型: 字符串

逗号分隔的 S3 存储桶名称列表，应为其启用数据事件日志记录。默认行为会检查所有 S3 存储桶。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloudtrail-security-trail-enabled

检查是否至少有一个为Amazon CloudTrail使用安全最佳实践定义跟踪。如果至少有一个跟踪满足以下所有条件，则此规则为合规：

- 记录全球服务事件
- 是一个多区域跟踪
- 启用了日志文件验证
- 使用 KMS 密钥加密
- 记录读取和写入事件
- 记录管理事件
- 不排除任何管理事件

如果跟踪均满足上述所有条件，则规则为 NON_COMPLIANT。

标识符：CLOUDTRAIL_SECURITY_TRAIL

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon区域，但亚太地区（雅加达）、亚太地区（大阪）区域除外

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloudwatch-alarm-action-check

检查是否 CloudWatch 警报至少启用了一个警报操作、一个INSUFFFICIENT_DATA 操作或一个正常操作。(可选) 检查是否有任何操作与指定的 ARN 之一匹配。

标识符：CLOUDWATCH_ALARM_ACTION_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

alarmActionRequired, 类型: 字符串, 默认值：True

警报具有至少一个操作。

insufficientDataAction必需, 类型: 字符串, 默认值：True

当警报从任意其他状态转换为 INSUFFFICIENT_DATA 状态时，警报至少有一个操作。

okActionRequired, 类型: 字符串, 原定设置值：false

当警报从任意其他状态转换为 OK状态时，警报至少有一个操作。

操作 1（可选）, 类型: 字符串

要执行的操作，指定为 ARN。

action2（可选）, 类型: 字符串

要执行的操作，指定为 ARN。

操作 3（可选）, 类型: 字符串

要执行的操作，指定为 ARN。

action4（可选）, 类型: 字符串

要执行的操作，指定为 ARN。

action5（可选）, 类型: 字符串

要执行的操作，指定为 ARN。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloudwatch-alarm-resource-check

检查指定的资源类型是否有针对性的 CloudWatch 针对指定指标的警报。对于资源类型，您可以指定 EBS 卷、EC2 实例、RDS 集群或 S3 存储桶。

标识符: CLOUDWATCH_ALARM_RESOUCE_CHECK

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

resourceType, 类型: 字符串

Amazon 资源类型。值可以是以下之一： AWS::EC2::Volume、 AWS::EC2::Instance、 AWS::RDS::DBCluster, or AWS::S3::Bucket.

metricName, 类型: 字符串

与警报关联的指标的名称 (例如，对于 EC2 实例为 “CPUtilization”)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloudwatch-alarm-settings-check

检查是否 CloudWatch 拥有指定指标名称的警报具有指定设置。

标识符：CLOUDWATCH_ALARM_设置_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

metricName, 类型: 字符串

　　与警报关联的指标的名称。
阈值（可选）, 类型：int

　　指定统计数据的比较值。
评估期（可选）, 类型：int

　　其间的数据将与指定阈值进行比较的期间数。
周期（可选）, 类型：int, 默认值：300

　　在其中应用指定统计数据的期间 (秒数)。
comparisonOperator（可选）, 类型: 字符串

　　比较指定的统计数据和阈值的操作 (例如，'GreaterThanThreshold')。
统计数据（可选）, 类型: 字符串

　　与警报关联的指标的统计数据 (例如，“平均值” 或 “总计”)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloud-trail-cloud-watch-logs 已启用

检查是否Amazon CloudTrail 配置了跟踪以将日志发送到 Amazon CloudWatch 日志。如果该跟踪不合规 CloudWatchLogsLogGroupArn 跟踪的属性为空。

标识符：CLOUD_TRAIL_CLOUD_WATCH_LOGS_已

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

expectedDeliveryWindow年龄（可选）, 类型：int

　　最近一次配送到的最长年龄（以小时为单位） CloudWatch 满足合规性的日志。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloudtrail-enabled

检查Amazon CloudTrail 已启用Amazonaccount. 或者，您也可以指定要使用的 S3 存储桶、SNS 主题和 Amazon CloudTrail ARN。如果 Amazon CloudTrail 未启用，则规则为 NON_COMPLIANT。

标识符：CLOUD_TRAIL_启用

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

s3BucketName （ 可选 ）, 类型: 字符串

的 S3 存储桶的名称 CloudTrail 将日志文件传送给。

snsTopicArn （ 可选 ）, 类型: 字符串

SNS 主题 ARN CloudTrail 使用提供通知服务。

cloudWatchLogsLogGroupArn （ 可选 ）, 类型: 字符串

CloudWatch 的日志组 ARN CloudTrail 将数据发送给。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloud-trail-encryption-enabled

检查 IANTAmazon CloudTrail配置为使用服务器端加密 (SSE)Amazon Key Management Service(Amazon KMS) 加密进行存储。如果规则为 COMPLIANT KmsKeyId 已定义。

标识符：CLOUD_TRAIL_加密_已启用

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cloud-trail-log-file-已启用验证

检查 Amazon CloudTrail 是否创建包含日志的签名摘要文件。Amazon 建议必须对所有跟踪启用文件验证。如果未启用验证，则规则为 NMPLIANT。

标识符：CLOUD_TRAIL_LOG_FILE_VALIDATION_已启用

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cmk-backing-key-rotation-启用

检查是否为每个启用了自动密钥轮替Amazon Key Management Service(Amazon KMS) 客户管理的对称加密密钥。如果没有为某启用自动密钥轮轮轮轮交换，则规则为 NON_COMPLIANTAmazon KMS客户管理的对称加密密钥。

> Note
>
> 在非对称 KMS 密钥、HMAC KMS 密钥、HMAC KMS 密钥、HMAC KMS 密钥中不受支持。

标识符：CMK_BACKING_KEY_ROTATION_已启用

触发器类型: 定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

codebuild-project-envvar-awscred-Check

检查项目是否包含环境变量Amazon_ACCESS_KEY_ID 和Amazon_SECRET_ACCESS_KEY。如果项目环境变量包含明文凭证，则规则为 NON_COMPLIANT。

标识符: CODEBUILD_PROJECT_ENVAR_AWSCRED_CHECK

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （美国东部）、亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

codebuild-project-source-repo-url-check

检查是否 GitHub 或 Bitbucket 源存储库 URL 包含个人访问令牌或用户名和密码。该规则与使用 OAuth 授予权限来访问 GitHub 或者 Bitbucket 存储库。

标识符 CODEBUILD_PROJECT_SOURCE_REPO_URL_CH

触发器类型 配置更改

Amazon Web Services 区域：全部支持Amazon除外区域Amazon GovCloud （美国东部）、亚太地区（亚太地区（亚太地区）、亚太地区（米兰）、亚太地区（米兰）、亚太地区（米兰）、亚太地区（亚太地区（亚太地区）

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

cw-loggroup-retention-period-check

检查亚马逊是否 CloudWatch LogGroup 保留期设置为特定的天数。如果日志组的保留期小于 NON_COMPLIANT MinRetentionTime 参数。

> Note
>
> 如果日志组的保留设置为 “永不过期”，则该规则将被标记为 “合规”。

标识符：CW_LOGGROUP_RETENTION_PERIOD_CHECK

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

LogGroupNames （可选），类型: CSV

日志组名称的逗号分隔的列表，用于检查保留期。

MinRetentionTime （可选），类型：int

指定保留时间。有效值为：
1、3、5、5、5、5、5、5、5、5、5、5、5、5、15、15、15、15、15、15、15、15、15、15、15、15、15、15
原定设置的保留期为 365 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

db-instance-backup-enabled

检查 RDS 数据库实例是否已启用备份。（可选）此规则将检查备份保留期和备份时段。

标识符: DB_INSTANCE_BACKUP_ENABLED

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

backupRetentionPeriod （可选）, 类型：int

备份的保留期。

backupRetentionMinimum （可选）, 类型：int

备份的最短保留期。

preferredBackupWindow （可选）, 类型: 字符串

创建备份的时间范围。

checkReadReplicas （可选）, 类型：布尔值

检查 RDS 数据库实例是否已针对只读副本启用备份。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

desired-instance-tenancy

检查实例的指定租期。指定 AMI ID 以检查从这些 AMI 启动的实例，或者指定主机 ID 以检查实例是否在这些专用主机上启动。用英文逗号分隔多个 ID 值。

标识符：DESIRED_INSTANCE_TENANCY

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

租期, 类型: 字符串

实例的期望租期。有效值为 “专用”、“主机” 和 “默认”。

imageId（可选）, 类型: CSV

规则仅评估从指定 ID 的 AMI 启动的实例。用英文逗号分隔多个 AMI ID。

hostId（可选）, 类型: CSV

专用主机的 ID，要在该主机上启动实例。用英文逗号分隔多个主机 ID。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

desired-instance-type

检查 EC2 实例是否具有指定的实例类型。

有关支持的 Amazon EC2 实例类型列表，请参阅实例类型中的Amazon EC2 Linux 用户指南.

标识符：DESIRED_INSTANCE_TYPE

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

instanceType, 类型: CSV

逗号分隔的 EC2 实例类型列表 (例如“t2.small, m4.large, i2.xlarge”)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

dms-replication-not-public

检查是否AmazonDatabase Migration Service 复制实例为公有实例。如果为 NON_COMPLIANT PubliclyAccessible 字段为 True。

标识符：DMS_REPLICATION_NOT_PUBLIC

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

dynamodb-autoscaling-enabled

检查是否在您的 DynamoDB 表和/或全局辅助索引上启用了 Auto Scaling 或按需功能。(可选) 您可以设置表或全局辅助索引的读取和写入容量单位。

标识符: DYNAMODB_AUTOSCALING_ENABLED

触发器类型: 定期

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud (US-East)、Amazon GovCloud （美国西部）区域

参数：

minProvisionedRead容量（可选）, 类型：int

应在 Auto Scaling 组中对读取容量配置的最小单位数。

maxProvisionedRead容量（可选），类型：int

应在 Auto Scaling 组中对写入容量配置的最小单位数。

targetReadUtilization （可选），类型：双精度

应在 Auto Scaling 组中对读取容量配置的最大单位数。

minProvisionedWrite容量（可选），类型：int

应在 Auto Scaling 组中对写入容量配置的最大单位数。

maxProvisionedWrite容量（可选），类型：int

读取容量的目标使用率百分比。目标使用率以占用容量与预置容量的比值来表示。

targetWriteUtilization （可选），类型：双精度

写入容量的目标使用率百分比。目标使用率以占用容量与预置容量的比值来表示。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

dynamodb-in-backup-plan

检查Amazon DynamoDB 表是否存在于AmazonBackup 计划。如果 Amazon DynamoDB 表中不存在 AmazonBackup 计划。

标识符：DYNAMODB_IN_BACKUP_PLAN

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （US-East）、Amazon GovCloud （US-East）、欧洲（米兰）、欧洲（米兰）、欧洲（米兰）、欧洲（米兰）、非洲（开普敦）、非洲（开普敦）、欧洲（

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

dynamodb-pitr-enabled

检查是否为 Amazon DynamoDB 表启用了时间点恢复 (PITR)。如果没有为 Amazon DynamoDB 表启用时间点恢复，则规则为 NON_COMPLIANT。

标识符：DYNAMODB_PITR_已启用

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太（雅加达）、亚太地区（大阪）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

dynamodb-table-encrypted-kms

检查 Amazon DynamoDB 表是否使用加密AmazonKMS KMS。如果 Amazon DynamoDB 表未使用加密，则规则为 NON_COMPLIANTAmazonKMS. 如果加密，则规则也是 NON_COMPLIANTAmazonKMS 密钥不存在于`kmsKeyArns`输入参数。

标识符：DYNAMODB_TABLE_ENCRYPTED_KMS

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon区域（大阪）以外的区域

参数：

kmsKeyArns （可选）, 类型: CSV

以逗号分隔的列表AmazonKMS Key ARN 允许加密 Amazon DynamoDB 表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

dynamodb-throughput-limit-check

检查为 DynamoDB 预配置的吞吐量是否正在接近账户最大限制。默认情况下，该规则检查预配置的吞吐量是否超过您的账户限制的阈值 (80%)。

标识符：DYNAMODB_吞吐量_LIMIT_CHECK

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域除外

参数：

账户 RCUThresholdPercentage （可选）, 类型：int, 默认值：80

为您的账户预配置的读取容量单位数的百分比。当达到此值时，将规则标记为 NON_COMPLIANT。

账户 WCUThresholdPercentage （可选）, 类型：int, 默认值：80

为您的账户预配置的写入容量单位数的百分比。当达到此值时，将规则标记为 NON_COMPLIANT。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ebs-in-backup-plan

检查Amazon Elastic Block Store (Amazon EBS) 卷是否已添加到AmazonBackup。如果 Amazon EBS 卷未包含在备份计划中，则规则为 NON_COMPLIANT。

标识符：EBS_IN_BACKUP_PLAN

触发器类型：Tri 定期

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （US-East）、Amazon GovCloud （US-East）、非洲（开普敦）、非洲（开普敦）、非洲（开普敦）、非洲（开普敦）、非洲（开普敦）、非洲（开普敦）

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ebs-optimized-instance

检查是否为可通过 EBS 优化的 EC2 实例启用 EBS 优化。如果未为可通过 EBS 优化的 EC2 实例启用 EBS 优化，则该规则为不合规。

标识符：EBS_OPTIMIZED_INSTAN

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ebs-snapshot-public-restorable-Check

检查Amazon Elastic Block Store (Amazon EBS) 快照是否不可公开恢复。如果包含一个或多个快照，则规则为 NON_COMPLIANT RestorableByUserIds 字段设置为全部，即 Amazon EBS 快照是公共的。

标识符：EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-ebs-encryption-by-default

检查默认情况下是否启用Amazon Elastic Block Store (EBS) 加密。如果未启用加密，则规则为 NON_COMPLIANT。

标识符：EC2_EBS_ENCRYPTION_BY_DEFAULT

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-imdsv2-check

检查您的亚马逊Elastic Compute Cloud (Amazon EC2) 实例元数据版本是否配置为 Instance Metadata Service Version 2 (IMDSv2)。如果为 NON_COMPLIANT HttpTokens 设置为可选。

标识符：EC2_IMDSV2_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-instance-detailed-monitoring-enabled

检查是否已为 EC2 实例启用详细监控。如果未启用详细监控，则该规则为 NON_COMPLIANT。

标识符：EC2_INSTANCE_DETAILED_MONITORING_ENABLED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-instance-managed-by-systems-Manager

检查您账户中的 Amazon EC2 实例是否由托管Amazon Systems Manager. 如果 Amazon EC2 实例已断开连接，则该规则为 NON_COMPLIANT。

标识符：EC2_INSTANCE_MANAGED_BY_SSM

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）区域以外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-instance-multiple-eni-check

检查Amazon EElastic Compute Cloud (Amazon EC2) e Compute Compute Compute Compute Compute Compute Compute 此规则不符合 Amazon EC2 实例使用多个网络接口。

标识符：EC2_INSTANCE_MULTIPLE_ENI_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （美国东部）、Amazon GovCloud (US-East)、亚太地区（雅加达）、亚太地区（大阪）区域

参数：

NetworkInterfaceIds （可选）, 类型: CSV

网络实例 ID 的逗号分隔列表

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-instance-no-public-ip

检查Amazon EElastic Compute Cloud (Amazon EC2) 实例是否有公有 IP 关联。如果 Amazon EC2 实例配置项中显示公有 IP 字段，则规则为 NON_COMPLIANT。此规则仅适用于 IPv4。

标识符：EC2_INSTANCE_NO_PUBLIC_IP

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-managedinstance-applications-blacklisted

检查实例上未安装指定的任何应用程序。(可选) 指定版本。较新的版本将不会被拒绝。根据需要指定平台，仅针对运行该平台的实例应用规则。

标识符：EC2_MANAGEDINSTANCE_APPLICATIONS_已列入黑名单

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（大阪）区域以外的地区

参数：

applicationNames, 类型: CSV

以逗号分隔的应用程序名称列表。(可选) 指定附加有 “:” 的版本 (例如，“Chrome: 0.5.3，FireFox”)。

Note

应用程序名称必须是完全匹配的。例如，在 Linux 上使用 **`firefox`** 或在 Amazon Linux 上使用 **`firefox-compat`**。此外，Amazon Config 目前不支持对 applicationNames 参数使用通配符（例如，**`firefox*`**）。

platformType（可选），类型: 字符串

平台类型 (例如，“Linux” 或 “Windows”)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-managedinstance-applications-required

检查实例上是否安装了所有指定应用程序。(可选) 指定可接受的最低版本。您还可以指定平台，仅针对运行该平台的实例应用规则。

Note

确保 SSM 代理在 EC2 实例上运行和创建关联以收集应用程序软件清单。如果未安装 SSM 代理或尚未创建或正在运行关联，则该规则返回 NOT_APPLIABLE。

标识符：EC2_MANAGEDINSTANCE_APPLICATIONS_必需

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（大阪）区域之外的区域

参数：

applicationNames, 类型: CSV

以逗号分隔的应用程序名称列表。(可选) 指定附加有 “:” 的版本 (例如，'Chrome: 0.5.3，Firefox ')。

Note

应用程序名称必须是完全匹配的。例如，在 Linux 上使用 **`firefox`** 或在 Amazon Linux 上使用 **`firefox-compat`**。此外，Amazon Config 目前不支持对 applicationNames 参数使用通配符（例如，**`firefox*`**）。

platformType（可选），类型: 字符串

平台类型 (例如，“Linux” 或 “Windows”)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-managedinstance-association-compliance-status-Check

检查状态是Amazon在实例上做了关联执行后，Systems Manager 关联合规性为 COMPLIANT。如果字段状态为 COMPLIANT，则规则为 COMPLIANT。有关关联的更多信息，请参阅什么是关联？.

标识符：EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域除外

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-managedinstance-inventory-blacklisted

检查由 Amazon EC2 系统托管的实例是否已配置为收集黑名单中的清单类型。

标识符：EC2_MANAGEDINSTANCE_INVENTORY_已列入黑名单

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（大阪）区域以外的地区

参数：

inventoryNames, 类型: CSV

以逗号分隔的 Systems Manager 清单类型列表（例如，'Amazon:网络、Amazon：WindowsUpdate')。

platformType（可选），类型: 字符串

平台类型 (例如，“Linux”)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-managedinstance-patch-compliance-status-Check

检查的合规性状态是Amazon在实例上安装补丁后，Systems Manager 合规性为 COMPLIANT 还是 NON_COMPLIANT。如果字段状态为 COMPLIANT，则规则为 COMPLIANT。

标识符: EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域外，其他区域（米兰）、中东（巴林）和非洲（开普敦）区域除外

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-managedinstance-platform-check

检查 EC2 托管实例是否具有所需的配置。

标识符: EC2_MANAGEDINSTANCE_PLATFORM_CHECK

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（大阪）区域以外区域

参数：

platformType, 类型: 字符串

平台类型 (例如，“Linux”)。

platformVersion（可选），类型: 字符串

平台版本（例如，'2016.09'）。

agentVersion（可选），类型: 字符串

代理版本 (例如，“2.0.433.0”)。

平台名称（可选），类型: 字符串

平台版本 (例如，“2016.09”)

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2security-group-attached-to-eni

检查非默认安全组是否附加到弹性网络接口 (ENI)。如果安全组未与elastic network interface (ENI) 相关联，规则将为 NON_COMPLIANT。

> Important
>
> 由于以下原因，此规则已被弃用间接关系淘汰因为间接关系一旦弃用，将不再创建触发此规则的配置项。如果您使用此规则，请将其从评估配置时删除Amazon资源并将其替换为新的ec2security-group-attached-to-eni-定期规则. 这些区域有：ec2security-group-attached-to-eni-定期规则不会受到此弃用的影响，因为它是定期触发的，而不是在配置更改时触发的。

标识符：EC2_SECURITY_GROUP_ATTACHED_TO_ENI

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-stopped-instance

检查是否有实例的停止时间超过了允许的天数。如果 ec2 实例的状态为已停止的时间超过了允许的天数，则该实例为 NON_COMPLIANT。

标识符：EC2_STOPPED_INSTANCE

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、亚太地区（大阪）、亚太地区（大阪）、亚太地区（大阪）、亚太地区（首尔首府）

参数：

AllowedDays （可选）, 类型：int, 默认值：30

ec2 实例在为 NON_COMPLIANT 之前可处于停止状态的天数。默认天数为 30。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-volume-inuse-check

检查 EBS 卷是否已附加到 EC2 实例。(可选) 检查 EBS 卷是否已标记为在实例终止时删除。

标识符: EC2_VOLUME_INUSE_CHECK

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

deleteOnTermination （ 可选 ）, 类型：布尔值

EBS 卷已标记为在实例终止时删除。可能的值：True 或 False（其他输入值被标记为不合规）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

efs-encrypted-check

检查是否将 Amazon Elastic File System (Amazon EFS) 配置为使用Amazon Key Management Service(Amazon KMS)。如果在 `DescribeFileSystems` 上将加密密钥设置为 false，或者 `DescribeFileSystems` 上的 `KmsKeyId` 密钥与 `KmsKeyId` 参数不匹配，则规则为 NON_COMPLIANT。

标识符：EFS_ENCRYPTED_CHECK

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域之外的区域

参数：

KmsKeyId （ 可选 ）, 类型: 字符串

用于加密 EFS 文件系统的 KMS 密钥的 Amazon 资源名称 (ARN)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

efs-in-backup-plan

检查 Amazon Elastic File System (Amazon EFS) 文件系统是否已添加到AmazonBackup。如果备份计划中未包括 EFS File System，则规则为 NOMPLIANT。

标识符: EFS_IN_BACKUP_PLAN

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除外区域Amazon GovCloud （美国东部）、Amazon GovCloud （美国西部）、非洲（米兰）、非洲（米兰）、非洲（开普敦）、非洲（开普敦）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

eip-attached

检查分配到的所有弹性 IP 地址Amazon账户已连接到 EC2 实例，还是正在使用的弹性网络接口 (ENI)。

> Note
>
> 评估发生后，可能需要最多 6 小时才能获得结果。

标识符：EIP_ATTACHED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

eks-endpoint-no-public-访问

检查Amazon Elastic Kubernetes Service (Amazon EKS) 终端节点是否不可公开访问。如果终端节点是可公开访问的，则规则为 NON_COMPLIANT。

标识符：EKS_ENDPOINT_NO_PUBLIC_ACC

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （美国东部）、Amazon GovCloud (US-西部)、亚太地区（大阪）、欧洲（大阪）、欧洲（大阪）、欧洲（开普敦）、欧洲（开普敦）、欧洲（开普敦）、欧洲（开普敦）、欧洲（开普敦）、

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

eks-secrets-encrypted

检查Amazon Elastic Kubernetes Service 集群是否配置为使用加密 Kubernetes 密钥Amazon Key Management Service(KMS) 密钥。

- 如果 EKS 集群具有将密钥作为资源之一的 EncryptionConfig，则此规则是合规的。
- 如果用于加密 EKS 密钥的密钥与参数匹配，则此规则也是合规的。
- 如果 EKS 集群没有 EncryptionConfig 或 EncryptionConfig 资源不包含机密，则此规则不合规。
- 如果用于加密 EKS 密钥与参数不匹配，则此规则也是 NON_COMPLIANT。

标识符：EKS_SECRETS_加密

Tri 定期

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、欧洲（加利福尼亚北部）、非洲（开普敦）以外的区域

参数：

kmsKeyArns （可选）, 类型: CSV

用逗号分隔的 KMS 密钥的 Amazon Resource Name (ARN)。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elasticache-redis-cluster-automatic-备份检查

检查亚马逊 ElastiCache Redis 集群已启用自动备份。当 SnapshotRetentionLimit 对于 Redis 群集小于 SnapshotRetentionPeriod 参数。例如：如果参数为 15，则当 snapshotRetentionPeriod 介于 0 至 15 之间时。

标识符：ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

snapshotRetentionPeriod （可选）, 类型：int, 默认值：15

Redis 集群的最短快照保留期（以天为单位）。默认值为 15 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elasticsearch-in-vpc-only

检查亚马逊是否 OpenSearch 服务 (OpenSearch Service)。Service Cloud (Amazon VPC)。如果规则为 NON_COMPLIANT OpenSearch 服务域终端结点是公有的。

标识符：ELASTICSEARCH_IN_VPC_ONLY

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除亚太 (雅加达)、亚太 (大阪)。

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elbv2-acm-certificate-required

检查应用程序负载均衡器和网络负载均衡器是否配置为使用来自Amazon Certificate Manager(ACM)。如果至少有 1 个负载均衡器至少有 1 个侦听器配置了没有 ACM 证书或配置了不同于 ACM 证书的证书，则此规则不合规。

标识符: ELBV2_ACM_CERTIFICATE_REQUIRED

触发器类型: 定期

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （美国东部）、Amazon GovCloud （美国西部）、亚太地区（雅加达）、亚太地区（大阪）区域

参数：

AcmCertificatesAllowed （可选）, 类型: CSV

证书的 Amazon 资源名称 (ARN) 的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elb-cross-zone-load-已启用平衡

检查是否为传统负载均衡器 (CLB) 启用跨区域负载均衡。如果未为 CLB 启用跨区域负载均衡，则规则为 NON_COMPLIANT。

标识符：ELB_CROSS_ZONE_LOAD_BALANCING_已启用

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elb-custom-security-policy-ssl-check

检查您的Classic Load Balancer SSL 侦听器是否在使用自定义策略。此规则只适用于有 Classic 负载均衡器有 SSL 侦听器的情况。

标识符：ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （美国东部）、亚太地区（大阪）、亚太地区（大阪）、亚太地区（大阪）、欧洲（开普敦）、亚太地区（大阪）、欧洲（开普敦）、亚

参数：

sslProtocolsAnd密码, 类型: 字符串

逗号分隔的密码和协议列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elb-deletion-protection-enabled

检查Elastic Load Balancing 是否启用了删除保护。如果 `deletion_protection.enabled` 为 false，则规则为 NON_COMPLIANT。

标识符：ELB_DELETION_保护_已启用

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elb-logging-enabled

检查Application Load Balancer Classic Load Balancer 是否启用了日志记录。如果规则为 NON_COMPLIANT`access_logs.s3.enabled`false 或`access_logs.S3.bucket`不等于 s3BucketName 你提供的。

标识符：ELB_LOGGING_ENABLED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

s3BucketNames （可选）, 类型: CSV

逗号分隔的 Amazon S3 存储桶名称列表，用于传送日志文件。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elb-predefined-security-policy-ssl-check

检查您的Classic Load Balancer SSL 侦听器是否在使用预定义策略。此规则只适用于有 SSL 侦听Classic Load Balancer。

标识符：ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （美国东部）、亚太地区（雅加达）、亚太地区（大阪）、亚太地区（米兰）、非洲（米兰）、亚太地区（开普敦）、亚太地区（亚太地区）

参数：

predefinedPolicyName, 类型: 字符串

预定义策略的名称。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

elb-tls-https-listeners-仅限

检查您的Classic Load Balancer 是否配置了 SSL 或 HTTPS 侦听器。

- 如果Classic Load Balancer 未配置侦听器，则规则返回 NOT_APPLIABLE。
- 如果Classic Load Balancer 侦听器配置了 SSL 或 HTTPS，则该规则是合规的。
- 如果监听器未配置 SSL 或 HTTPS，则规则为 NON_COMPLIANT。

标识符: ELB_TLS_HTTPS_LISTENERS_ONLY

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon区域（雅加达）、亚太地区（大阪）、亚太地区（大阪）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

emr-kerberos-enabled

检查 Amazon EMR 集群是否启用了 Kerberos。如果未将安全配置附加到群集或安全配置不满足指定的规则参数，则规则为 NON_COMPLIANT。

标识符: EMR_KERBEROS_已启用

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon亚太（雅加达）、亚太地区（大阪）、

参数：

TicketLifetimeInHours （可选）, 类型：int

群集 KDC 签发的 Kerberos 票证的有效期。

领域（可选）, 类型: 字符串

信任关系中另一领域的 Kerberos 领域名称。

Domain（可选）, 类型: 字符串

信任关系中另一领域的域名。

AdminServer （可选）, 类型: 字符串

信任关系的另一领域中的管理服务器的完全限定域名。

KdcServer （可选）, 类型: 字符串

信任关系的另一领域中的 KDC 服务器的完全限定域名。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

emr-master-no-public-ip

检查 Amazon Amazon MapReduce (EMR) 集群的主节点具有公有 IP。如果主节点具有公有 IP，则该规则为 NON_COMPLIANT。

Note

此规则检查处于 RUNNING 或 WAITING 状态的集群。

标识符：EMR_MASTER_NO_PUBLIC_IP

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域除外

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

encrypted-volumes

检查处于连接状态的 EBS 卷是否已加密。如果使用 kmsId 参数为加密指定了 KMS 密钥的 ID，则该规则将检查连接状态中的 EBS 卷是否使用该 KMS 密钥进行加密。

标识符：加密卷

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域除外的地区

参数：

kmsId (可选), 类型: 字符串

用于加密卷的 KMS 密钥的 ID 或 ARN。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

fms-webacl-resource-policy-Check

检查 Web ACL 是否与Application Load Balancer、API Gateway 阶段或 Amazon 相关联 CloudFront 分配。当 Amazon Firewall Manager 创建此规则时，FMS 策略所有者会在 FMS 策略中指定 `WebACLId`，并且可选择启用补救功能。

标识符：FMS_WEBACL_RESOURCE_POLICY_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）区域之外的区域

参数：

webACLId, 类型: 字符串

Web ACL 的 WebACLId。

resourceTags（可选）, 类型: 字符串

资源标签 (ApplicationLoadBalancer、 ApiGatewayStage 和 CloudFront 分配），规则应与之关联。（例如，{“tagValue1": [" tagValue1": ["tagValue3": [" tagValue3": ["tagValue3"]})

excludeResourceTags（可选）, 类型：布尔值

如果为 true，则排除与 resourceTags 匹配的资源。

fmsManagedToken（可选）, 类型: 字符串

生成的令牌Amazon当在客户帐户中创建规则时，Firewall Manager。Amazon当客户创建此规则时，Config 会忽略此参数。

fmsRemediationEnabled（可选）, 类型：布尔值

如果为 true，AmazonFirewall Manager 将根据 FMS 策略更新不合规资源。Amazon当客户创建此规则时，Config 会忽略此参数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

fms-webacl-rulegroup-association-check

检查规则组是否与处于正确优先级的 Web ACL 关联。正确优先级由规则组在 ruleGroups 参数中的排名决定。当 Amazon Firewall Manager 创建此规则时，它会分配最高优先级 0，再分配 1、2，以此类推。FMS 策略所有者在 FMS 策略中指定 `ruleGroups` 排名，并且可以选择启用补救功能。

标识符：FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）区域之外的地区

参数：

ruleGroups, 类型: 字符串

以逗号分隔的 RuleGroupIds 和 WafOverrideAction 对。 （例如， ruleGroupId-1: 无， ruleGroupId2: COUNT)

fmsManagedToken （可选）, 类型: 字符串

生成的令牌Amazon当在客户帐户中创建规则时，Firewall Manager。Amazon当客户创建此规则时，Config 会忽略此参数。

fmsRemediationEnabled （可选）, 类型：布尔值

如果为 true，AmazonFirewall Manager 将根据 FMS 策略更新不合规资源。Amazon当客户创建此规则时，Config 会忽略此参数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-customer-policy-blocked-kms-actions

检查是否托管Amazon您创建Identity and Access Management (IAM) 策略不允许对执行阻止操作AmazonKMS 密钥。如果允许执行任何阻止操作，则规则为 NON_COMPLIANTAmazon托管 IAM 策略提供的 KMS 密钥。

Note

此规则不评估 IAM 策略中提供的条件。有关 IAM 条件的更多信息，请参阅IAM JSON 策略元素：Condition(在 IAM 用户指南中)。

标识符：IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太 (雅加达)、亚太 (大阪) 区域之外的区域

参数：

blockedActionsPatterns, 类型: CSV

阻止的 KMS 操作模式的逗号分隔列表，例如，kms: *、KMS: Decrypt、kms:ReEncrypt*。

excludePermissionBoundary策略（可选）, 类型：布尔值

布尔标志，用于排除用作权限边界的 IAM 策略的评估。如果设置为 “true”，则该规则将不会在评估中包含权限边界。否则，当值设置为 “false” 时，将评估范围内的所有 IAM 策略。默认值为'false'。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-group-has-users-Check

检查 IAM 组是否至少拥有一个 IAM 用户。

标识符：IAM_GROUP_HAS_USERS_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-inline-policy-blocked-kms-actions

检查附加到您的 IAM 用户、角色和组的内联策略是否不允许对所有 IAM 用户、角色和组执行阻止的操作 AmazonKey Management Key Key。如果允许对内联策略中的所有 KMS Key 执行任何阻止操作，则规则为 NON_COMPLIANT。

标识符：IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、亚太地区（大阪）区域除外

参数：

blockedActionsPatterns, 类型: CSV

阻止的 KMS 操作模式的逗号分隔列表，例如，kms: *、KMS: Decryt、kms: Decryt、kms: kms:ReEncrypt*。

excludeRoleByManagementAccount （可选），类型：布尔值

如果角色只能由组织管理账户承担，则排除该角色。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-no-inline-policy-Check

检查是否未使用内联策略功能。如果为AmazonIdentity and Accccccess Management (IAM) 用户、IAm角色或 IAccc

标识符：IAM_NO_INLINE_POLICY_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太 (雅加达)、亚太 (大阪)、亚太 (大阪) 区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-password-policy

检查 IAM 用户的账户密码策略是否符合参数中指示的指定要求。如果账户密码策略不符合指定要求，则规则为 NON_COMPLIANT。

> Note
>
> 使用默认 IAM 密码策略时，该规则将被标记为不合规。
>
> Important
>
> 这些区域有：`true`和`false`规则参数的值区分大小写。如果`true`未提供小写字母，它将被视为`false`.

标识符：IM_PASSWORD_POLICY

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

RequireUppercaseCharacters （可选），类型：布尔值, 默认值：True

密码中要求至少包含一个大写字符。

RequireLowercaseCharacters （可选），类型：布尔值, 默认值：True

密码中要求至少包含一个小写字符。

RequireSymbols （可选），类型：布尔值, 默认值：True

密码中要求至少包含一个符号。

RequireNumbers （可选），类型：布尔值, 默认值：True

密码中要求至少包含一个数字。

MinimumPasswordLength （可选），类型：int, 默认值：14

密码最小长度。

PasswordReusePrevention （可选），类型：int, 默认值：24

允许重用前的密码数。

MaxPasswordAge （可选），类型：int, 默认值：90

密码到期前的天数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-policy-blacklisted-check

检查对于每个 IAM 资源，输入参数中的策略 ARN 是否附加到 IAM 资源。如果策略 ARN 附加到 IAM 资源，则规则为 NON_COMPLIANT。Amazon Config如果 IAM 资源是`exceptionList`参数，而不考虑策略 ARN 是否存在。

标识符：IAM_POLICY_BLACKLISTED_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

policyArns, 类型: CSV, 默认:aws: iam: aws: iam: aws: policy/AdministratorAccess

逗号分隔的 IAM 策略 arn 列表，不应附加到任何 IAM 实体。

exceptionList（可选）, 类型: CSV

此规则免除的用户、组或角色的逗号分隔列表。例如，users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3]。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-policy-in-use

检查 IAM 策略 ARN 是否附加到 IAM 用户，是否附加到 IAM 用户，或者是否附加到 IAM 具有一个或多个可信实体的组，或者是否附加到 IAM 角色。

标识符: IAM_POLICY_IN_USE

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域除外

参数：

PpolicyARN, 类型: 字符串

要检查的 IAM 策略 ARN。

policyUsageType （可选）, 类型: 字符串

指定是否希望策略附加到 IAM 用户、组或角色。有效值为 IAM_USER、IAM_GROUP、IAM_ROLE 或 ANY。默认值为 ANY。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-policy-no-statements-with-admin-access

检查您为 Allow 语句创建的 IAM 策略，不得用 Allow 语句将权限授予所有资源上的所有操作。如果任何策略语句具有 “Efffect”: Effect”: Effect”: Allow”: “*” 上方包含 “Resource”: “*” 上方包含 “Action”: “*")

以下策略为 NON_COMPLIANT：

```
"Statement": [
{
"Sid": "VisualEditor",
```

```
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

以下策略合规：

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

此规则仅检查您创建的 IAM 策略。它不检查 IAM 托管策略。在您启用规则时，此规则将检查您账户中的所有客户管理策略以及您创建的所有新策略。

标识符符: IM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

触发器类型:Tri 配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-role-managed-policy-Check

检查是否全部Amazon托管策略列表中指定的托管策略将附加到AmazonIdIdentity and Access Management (IAM) cc 如果出现以下情况，则该规则不合规Amazon托管策略未附加到 IAM 角色。

标识符: IAM_ROLE_MANAGED_POLICY_CHECK

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

managedPolicyArns, 类型: CSV

的逗号分隔列表Amazon托管策略 ARN。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-root-access-key-check

检查 root 用户访问密钥是否可用。如果用户访问密钥不存在，则规则为 COMPLIANT。否则，不合规。

标识符：IAM_ROOT_ACCESS_KEY_CHECK

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon区域（亚太地区（雅加达）、亚太地区（大阪）区域除外

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-user-group-membership-check

检查 IAM 用户是否为至少一个 IAM 组的成员。

标识符: IAM_USER_GROUP_MEMBERSHIP_CHECK

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

组名（可选）, 类型: 字符串

IAM 用户必须是其成员的 IAM 组的逗号分隔列表。

Note

此规则不支持带有逗号的组名。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-user-mfa-enabled

检查是否AmazonIdentity and Access Management 用户启用了多重验证 (MFA)

标识符：IAM_USER_MFA_已启用

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-user-no-policies-Check

检查您的所有 IAM 用户均没有附加策略。IAM 用户必须继承来自 IAM 组或角色的权限。如果至少有一个 IAM 用户附加了策略，则该规则不合规。

标识符：IAM_USER_NO_POLICIES_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

iam-user-unused-credentials-Check

检查您的Amazon Identity and Access Management(IAM) 用户拥有在您提供的指定天数内尚未使用的密码或活动访问密钥。如果存在最近尚未使用的活动帐户，则规则为 NON_COMPLIANT。

> Note
>
> 在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。

标识符: IAM_USER_UNUSED_CREDENTIALS_CHECK

触发器类型: 定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

maxCredentialUsageAge, 类型：int, 默认值：90

必须使用凭证的最大天数。默认值为 90 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

restricted-ssh

检查安全组的传入 SSH 流量是否可访问。当安全组中的传入 SSH 流量的 IP 地址受限时（CIDR 不是 0.0.0.0/0），规则为 COMPLIANT。此规则仅适用于 IPv4。

标识符号：INCOMING_SSH_DISABLED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域之外的地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ec2-instances-in-vpc

检查您的 EC2 实例是否属于某个 Virtual Private Cloud (VPC)。或者，您可以指定要与您的实例关联的 VPC ID。

标识符: INSTANCES_IN_VPC

Triger: 配置更改

Amazon Web Services 区域：全部支持Amazon区域中亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域除外

参数：

vpcId（可选）, 类型: 字符串

包含这些 EC2 实例的 VPC ID。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

internet-gateway-authorized-vpc-限

检查是否仅将互联网网关 (IGW) 附加到授权 Amazon Virtual Private Cloud (VPC)。如果 IGW 未附加到授权 VPC，则规则为 NON_COMPLIANT。

标识符: 互联网网关_AUTHORIZED_VPC_ONLY

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域以外的区域

参数：

AuthorizedVpcIds （可选）, 类型: 字符串

带有附加 iGW 的授权 VPC ID 的逗号分隔列表。如果未提供此参数，则所有附加的 IGW 将为 NON_COMPLIANT。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

kms-cmk-not-scheduled-for delete

检查是否Amazon KMS keys未计划删除Amazon Key Management Service(Amazon KMS)。如果计划删除 KMS 密钥，则规则为 NON_COMPLIANT。

标识符: KMS_CMK_NOT_SCHEDULED_FOR_DELETION

触发器类型: 定期

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）区域除外

参数：

kmsKeyIds （可选）, 类型: 字符串

（可选）未计划删除的特定客户托管密钥 ID 的逗号分隔列表。如果未指定任何密钥，则规则将检查所有密钥。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

mfa-enabled-for-iam-控制台访问权限

检查是否Amazon为所有人启用Multi-Factor Authentication (MFA)Amazon使用控制台密码的Identity and Access Management (IAM) 用户。如果已启用 MFA，则规则为 COMPLIANT。

标识符: MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

multi-region-cloudtrail-enabled

检查是否至少有一个多区域Amazon CloudTrail. 如果跟踪与输入参数不匹配，则规则为 NON_COMPLIANT。如果为 NON_COMPLIANT`ExcludeManagementEventSources`字段不为空或者如果Amazon CloudTrail 配置为排除管理事件，例如Amazon KMS事件或 Amazon RDS 数据 API 事件。

标识符：多区域_CLOUD_TRAIL_已启用

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

s3BucketName （可选）, 类型: 字符串

Amazon S3 存储桶的名称Amazon CloudTrail 将日志文件传送给。

snsTopicArn （可选）, 类型: 字符串

Amazon SNS 主题 ARN 为Amazon CloudTrail 将使用提供通知服务。

cloudWatchLogsLogGroupArn （ 可选 ）, 类型: 字符串

亚马逊 CloudWatch 的日志组 ARNAmazon CloudTrail 将数据发送给。

includeManagementEvents （ 可选 ）, 类型：布尔值

要包含 Amazon CloudTrail 的管理事件的事件选择器。

readWriteType （ 可选 ）, 类型: 字符串

要记录的事件的类型。有效值为 ReadOnly、 WriteOnly 和所有。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

rds-enhanced-monitoring-enabled

检查是否为 Amazon Relational Database Service (Amazon RDS) 实例启用了增强监控。

标识符：RDS_ENHANCED_MONITORING_ENABLED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon区域，亚太 (雅加达) 区域除外

参数：

monitoringInterval（ 可选 ）, 类型：int

一个整数值，表示为数据库实例收集增强监控指标时，点之间的秒数。有效值为 1、5、10、15、30 和 60。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

rds-instance-deletion-protection-已启用

检查Amazon Relational Database Service (Amazon Relational Databas 如果 Amazon RDS 实例未启用删除保护，则此规则不合规，即`deletionProtection`设置为 false。

Warning

集群（Aurora/DocumentDB）中的某些 RDS 数据库实例将显示为不合规。

标识符：RDS_INSTANCE_DELETION_PROTECTION_已启用

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

数据库引擎（ 可选 ）, 类型: CSV

要包含在规则评估中的 Relational Database Relational DS Relational Database R 例如，'mysql、postgres、mariadb'。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

rds-instance-public-access-Check

检查实例是否可公开访问 Amazon Relational Database Service。如果实例配置项中的 `publiclyAccessible` 字段为 true，则规则为 NON_COMPLIANT。

标识符: RDS_INSTANCE_PUBLIC_ACCESS_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

rds-in-backup-plan

检查 Amazon RDS 数据库是否存在于的后期计划中AmazonBackup 如果 Amazon RDS 数据库未包含在任何规则中，则规则为 NON_COMPLIANTAmazonBackup 计划。

标识符: RDS_IN_BACKUP_PLAN

触发器类型: 定期

Amazon Web Services 区域：全部支持Amazon除外的地区Amazon GovCloud （美国东部）、Amazon GovCloud （美国西部）、亚太地区（雅加达）、亚太地区（香夏）、亚太地区（米兰）和非洲（米兰）、非洲（米兰）和非洲（米兰）

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

rds-multi-az-support

检查您的 RDS 数据库实例是否启用了高可用性。

在多可用区部署中，Amazon RDS 会自动在不同可用区中配置和维护一个同步备用副本。有关更多信息，请参阅 。高可用性（多可用区）中的Amazon RDS 用户指南.

> **Note**
>
> 此规则不评估Amazon Aurora 数据库和 Amazon DocumentDB 实例。

标识符：RDS_MULTI_AZ_SUPPORT

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

rds-snapshots-public-prohibited

检查Amazon Relational Database Service（Amazon RDS 如果任何现有的 Amazon RDS 快照都是公有的，则规则为 NON_COMPLIANT。

> Note
>
> 系统最长可能需要在 12 小时后才会捕获合规性结果。

标识符：RDS_SNAPSHOTS_PUBLIC_禁止

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）、亚太地区（大阪）、欧洲（开普敦）、亚太

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

rds-snapshot-encrypted

检查是否已加密 Amazon Relational Database Service (Amazon R 如果 Amazon RDS Database 快照未加密，则规则为 NON_COMPLIANT。

标识符：RDS_SNAPSHOT_已加密

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

rds-storage-encrypted

检查您的 RDS 数据库实例是否启用了存储加密。

标识符：RDS_STORAGE_已加密

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

kmsKeyId （可选）, 类型: 字符串

用于加密存储的 KMS 密钥 ID 或 ARN。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

redshift-cluster-configuration-check

检查 Amazon Redshift 集群是否具有指定的设置。

标识符：REDSHIFT_CLUSTER_CONFIGURATION_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon中东（巴林）区域之外的区域

参数：

clusterDbEncrypted, 类型：布尔值, 默认值：True

数据库加密已启用。

loggingEnabled, 类型：布尔值, 默认值：True

审核日志记录已启用。

nodeTypes（可选）, 类型: CSV, 默认值：dc1.large

指定节点类型。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

redshift-cluster-maintenancesettings-check

检查 Amazon Redshift 集群是否具有指定的维护设置。

标识符：REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon中东（巴林）区域以外的区域

参数：

allowVersionUpgrade, 类型：布尔值, 默认值：True

允许版本升级已启用。

preferredMaintenanceWindow （ 可选 ）, 类型: 字符串

为集群计划的维护时段 (例如，周一 09:30 - 周一 10:00)。

automatedSnapshotRetention句点（ 可选 ）, 类型：int, 默认值：1

自动快照要被保留的天数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

redshift-cluster-public-access-check

检查Amazon Redshift 集群是否可公开访问。如果集群配置项中的 `publiclyAccessible` 字段为 true，则规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon区域（ 雅加达 ）、亚太地区（ 大阪 ）、亚太地区（ 大阪 ）、

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

redshift-require-tls-ssl

检查Amazon Redshift 集群是否需要 TLS/SL 加密才能连接到 SQL 客户端。如果任何 Amazon Redshift yger tyger tyger tyger tyger tyger tyger tyger tyger

标识符：REDSHIFT_REQUIRE_TLS_SSL

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（ 雅加达 ）、亚太地区（ 大阪 ）、欧洲（ 米兰 ）区域之外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

required-tags

检查您的资源是否具有您指定的标签。例如，您可以检查 Amazon ec2 实例是否具有`CostCenter`标记。用英文逗号分隔多个值。您一次最多可以检查 6 个标签。

这些区域有：Amazon-管理Amazon Systems Manager自动化文档`AWS-SetRequiredTags`不能用作此规则的补救措施。您需要创建自己的自定义 Systems Manager 自动化文档以进行补救。

> Important
>
> 此规则支持的资源类型如下所示：
>
> - ACM::Certificate
> - AutoScaling::AutoScalingGroup
> - CloudFormation:: 堆叠
> - CodeBuild：项目
> - DynamoDB::Table
> - EC2::CustomerGateway
> - EC2::Instance
> - EC2::InternetGateway
> - EC2::NetworkAcl
> - EC2::NetworkInterface
> - EC2::RouteTable
> - EC2::SecurityGroup
> - EC2::Subnet
> - EC2::Volume
> - EC2::VPC
> - EC2::VPNConnection
> - EC2::VPNGateway
> - ElasticLoadBalancing::LoadBalancer
> - ElasticLoadBalancingV2::LoadBalancer
> - RDS::DBInstance
> - RDS:: DBSecurityGroup
> - RDS::DBSnapshot
> - RDS:: DBSubnetGroup
> - RDS:EventSubscription
> - Redshift::Cluster
> - Redshift::ClusterParameterGroup
> - Redshift::ClusterSecurityGroup
> - Redshift::ClusterSnapshot
> - Redshift::ClusterSubnetGroup
> - S3::Bucket

标识符：REQUIRED_TAGS

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

tag1Key, 类型: 字符串, 默认值： CostCenter

所需标签的键。

tag1Valuze（可选）, 类型: CSV

所需标签的可选值。用英文逗号分隔多个值。

tag2key（可选）, 类型: 字符串

所需标签的键。

tag2Value（可选）, 类型: CSV

所需标签的可选值。用英文逗号分隔多个值。

tag3key（可选）, 类型: 字符串

所需标签的键。

tag3Value（可选）, 类型: CSV

所需标签的可选值。用英文逗号分隔多个值。

tag4key（可选）, 类型: 字符串

所需标签的键。

tag4Value（可选）, 类型: CSV

所需标签的可选值。用英文逗号分隔多个值。

tag5key（可选）, 类型: 字符串

所需标签的键。

tag5Value（可选）, 类型: CSV

所需标签的可选值。用英文逗号分隔多个值。

tag6Key（可选）, 类型: 字符串

所需标签的键。

tag6Value（可选）, 类型: CSV

所需标签的可选值。用英文逗号分隔多个值。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

restricted-common-ports

检查所用安全组是否不允许受限传入 TCP 流量进入指定的端口。当入站 TCP 连接的 IP 地址限制为指定端口时，规则为 COMPLIANT。此规则仅适用于 IPv4。

标识符：受限_传入_流量

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、非洲（开普敦）区域除外

参数：

BlockedPort1（可选），类型：int, 默认值：20

已阻止的 TCP 端口号。

BlockedPort2（可选），类型：int, 默认值：21

已阻止的 TCP 端口号。

BlockedPort3（可选），类型：int, 默认值：3389

已阻止的 TCP 端口号。

BlockedPort4（可选），类型：int, 默认值：3306

已阻止的 TCP 端口号。

BlockedPort5（可选），类型：int, 默认值：4333

已阻止的 TCP 端口号。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-account-level-public-access-块

检查是否从账户级别配置了所需的公有访问块设置。仅当下面设置的字段与配置项中的相应字段不匹配时，该规则才为 NON_COMPLIANT。

Note

如果您正在使用此规则，请确保已启用 S3 阻止公有访问。该规则是更改触发的，因此除非启用 S3 阻止公共访问，否则不会调用该规则。如果未启用 S3 阻止公共访问，则规则将返回 INSUFFICIENT_DATA。这意味着你可能还有一些公共存储桶。有关设置 S3 阻止公有访问的更多信息，请参阅阻止对您的 Amazon S3 存储的公有访问.

标识符：S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BL

触发器类型：配置更改（未选中当前状态，仅在更改生成新事件时进行评估）

Note

此规则仅在 S3 终端节点所在的特定区域的配置更改时触发。在所有其他区域，会定期检查该规则。如果在其他区域进行了更改，则在规则返回 NON_COMPLITABLY 之前可能会有一段延迟。

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）、亚太地区（大阪）、欧洲（米兰）、中东（巴林）区域除外

参数：

IgnorePublicAcls（可选），类型: 字符串, 默认值：True

IgnorePublicAcls 是否强制执行，默认为 True

BlockPublicPolicy（可选），类型: 字符串, 默认值：True

BlockPublicPolicy 是否强制执行，默认为 True

BlockPublicAcls（可选），类型: 字符串, 默认值：True

BlockPublicAcls 是否强制执行，默认为 True

RestrictPublicBuckets（可选），类型: 字符串, 默认值：True

RestrictPublicBuckets 是否强制执行，默认为 True

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-blacklisted-actions-prohibited

检查 Amazon Simple Storage Service 存储桶策略是否不允许其他委托人对存储桶中的资源进行黑名单上的存储桶级和对象级操作。Amazon账户。例如，该规则检查 Amazon S3 存储桶策略是否不允许另一个 Amazon账户来执行任何 s3:GetBucket* 操作和 s3:DeleteObject 存储桶中的任何对象。如果 Amazon S3 存储桶策略允许任何列入黑名单的操作，则规则为 NON_COMPLIANT。

标识符: S3_BUCKET_BLACKLISTED_ACTIONS_禁止

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

blacklistedActionPattern, 类型: CSV

列入黑名单的操作模式的逗号分隔列表，例如，s3:GetBucket* 和 s3:DeleteObject.

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-default-lock-enabled

默认情况下，检查 Amazon S3 存储桶是否启用了锁定。如果锁定未启用，则规则为 NON_COMPLIANT。

标识符: S3_BUCKET_DEFAULT_LOCK_ENABLED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

mode（可选）, 类型: 字符串

模式:（可选）：具有 GOVERNANCE 或 COMPLIANCE 有效值的模式参数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-logging-enabled

检查您的 S3 存储桶是否已启用日志记录。

标识符: S3_BUCKET_LOGGING_ENABLED

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

targetBucket（可选），类型: 字符串

用于存储服务器访问日志的目标 S3 存储桶。

targetPrefix（可选），类型: 字符串

用于存储服务器访问日志所用的 S3 存储桶的前缀。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-policy-grantee-check

检查 Amazon S3 存储桶授予的访问权限是否受任何Amazon委托人、您提供的 VPC 地址或您提供的 VPC 如果存储桶策略不存在，则规则为 COMPLIANT。

例如，如果规则的输入参数为包含 111122223333 和 444455556666 这两个委托人的列表，并且存储桶策略指定仅 111122223333 能够访问存储桶，则规则为 COMPLIANT。使用相同的输入参数：如果存储桶策略指定111122223333和444455556666可以访问存储桶，它也是合规的。但是，如果存储桶策略指定 999900009999 可以访问存储桶，则规则将为 NON-COMPLIANT。

> Note
>
> 如果存储桶策略包含多条语句，则会根据此规则评估存储桶策略中的每条语句。

标识符：S3_BUCKET_POLICY_GRANTEE_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

awsPrincipals（可选），类型: CSV

委托人 ARN 和委托人 ARN 等委托人 ARN 和委托人 ARN 等委托人 ARN 和委托人 ARNAmazon账户，例如 “iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam: iam

servicePrincipals（可选），类型: CSV

服务委托人的逗号分隔列表，例如 “cloudre.iams.com”。

federatedUsers（可选），类型: CSV

Web 联合身份提供商（例如 Amazon Cognito 和 SAML 身份提供商）的逗号分隔列表。例如 “arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn: arn:

ipAddresses s（可选），类型: CSV

以逗号分隔的 CIDR 格式的 IP 地址列表，例如 '10.0.0.1、192.168.1.0/24、2001: db8:: /32'。

vpcIds（可选），类型: CSV

亚马逊虚拟私有云 (Amazon VPC) ID 的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-policy-not-more-宽容

检查您的 Amazon S3 存储桶策略是否不允许您提供的控制 Amazon S3 存储桶策略之外的其他账户间权限。

> Note
>
> 如果您提供了无效的参数值，则将看到以下错误：controlPolicy 参数的值必须是 Amazon S3 存储桶策略。

标识符：S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

controlPolicy, 类型: 字符串

> 定义您的 S3 存储桶的权限上限的 Amazon S3 存储桶策略。此策略的最大长度为 1024 个字符。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3.bucket-public-read-prohibited

检查您的 Amazon S3 存储桶是否允许公有读取访问。该规则将检查“阻止公有访问”设置、存储桶策略和存储桶访问控制列表 (ACL)。

当满足以下两个条件时，该规则也合规：

- “阻止公有访问”设置限制公有策略，或者存储桶策略不允许公有读取访问。
- “阻止公有访问”设置限制公有 ACL，或者存储桶 ACL 不允许公有读取访问。

在以下情况下，该规则不合规：

- 如果 “阻止公有访问” 设置不限制公有策略，则Amazon Config评估策略是否允许公有读取访问。如果策略允许公有读取访问，则该规则不合规。
- 如果 “阻止公有访问” 设置不限制公有存储桶 ACL，则Amazon Config评估存储桶 ACL 是否允许公有读取访问。如果存储桶 ACL 允许公有读取访问，则规则将不合规。

> Note
>
> 此规则不评估账户级别公共封禁访问权限的更改。要检查是否从账户级别配置了所需的公有访问块设置，请参阅s3.account-level-public-access-块和s3.account-level-public-access-blocks-周期性.

标识符：S3_BUCKET_PUBLIC_READ_PROBILEDED

触发器类型：配置更改和定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3bucket-public-write-prohibited

检查您的 Amazon S3 存储桶是否允许公有写入访问。该规则将检查“阻止公有访问”设置、存储桶策略和存储桶访问控制列表 (ACL)。

当满足以下两个条件时，该规则也合规：

- “阻止公有访问”设置限制公有策略，或者存储桶策略不允许公有写入访问。
- “阻止公有访问”设置限制公有 ACL，或者存储桶 ACL 不允许公有写入访问。

在以下情况下，该规则不合规：

- 如果 “阻止公有访问” 设置不限制公有策略，则Amazon Config评估策略是否允许公共写入访问。如果策略允许公有写入访问，则该规则不合规。
- 如果 “阻止公有访问” 设置不限制公有存储桶 ACL，则Amazon Config评估存储桶 ACL 是否允许公共写入访问。如果存储桶 ACL 允许公有写入访问，则规则将不合规。

> **Note**
>
> 此规则不评估账户级别公共封禁访问权限的更改。要检查是否从账户级别配置了所需的公有访问块设置，请参阅s3account-level-public-access-块和s3account-level-public-access-blocks-周期性.

标识符: S3_BUCKET_PUBLIC_WRITE_PROBILEDED

触发器类型：配置更改和定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-replication-enabled

检查 Amazon S3 存储桶是否启用了跨区域复制。

标识符: S3_BUCKET_REPLICATION_已启用

触发器类型: 配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-server-side-encryption-已启用

检查您的 Amazon S3 存储桶是否启用了 Amazon S3 默认加密，或检查 Amazon S3 存储桶策略是否明确拒绝该加密`put-object`不使用服务器端加密的请求使用 AES-256 或Amazon Key Management Service. 如果 Amazon S3 存储桶默认未加密，则规则为 NON_COMPLIANT。

标识符：S3_BUCKET_SERVER_SIDE_ENCRYPTION_已启用

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-ssl-requests-only

检查 Amazon S3 存储桶是否具有需要请求使用安全套接字层 (SSL) 的策略。如果存储桶明确拒绝对 HTTP 请求的访问，则规则为 COMPLIANT。如果存储桶策略允许 HTTP 请求，则规则为 NON_COMPLIANT。

标识符：S3_BUCKET_SSL_REQUESTS_ONLY

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-bucket-versioning-enabled

检查您的 S3 存储桶是否已启用版本控制。(可选) 该规则检查是否为您的 S3 存储桶启用了 MFA 删除。

标识符：S3_BUCKET_VERSIONING_已启用

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon地区

参数：

isMfaDelete已启用（可选），类型: 字符串

已经为您的 S3 存储桶启用了 MFA 删除。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

s3-default-encryption-kms

检查 Amazon S3 存储桶是否使用加密AmazonKey ManagementAmazonKMS). 如果 Amazon S3 存储桶未使用加密，则规则为 NON_COMPLIANTAmazonKMS 密钥。

标识符：S3_DEFAULT_ENCRYPTION_KMS

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域以外的区域

参数：

kmsKeyArns （可选），类型: CSV

以逗号分隔的列表AmazonKMS 密钥 ARN 允许加密 Amazon S3 存储桶。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

secretsmanager-rotation-enabled-check

检查是否AmazonSecrets Manager 密钥已启用轮换。此外，该规则还检查可选 `maximumAllowedRotationFrequency` 参数。如果指定了参数，则密钥的轮换频率与允许的最大频率进行比较。如果密钥未计划轮换，则规则为 NON_COMPLIANT。如果轮换频率高于maximumAllowedRotation频率参数。

Note

在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。

标识符：SECRETSMANAGER_ROTATION_ENABLED_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域之外的区域

参数：

maximumAllowedRotation频率（可选），类型：int

密钥允许的最大轮换频率（以天为单位）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

secretsmanager-scheduled-rotation-success-check

检查是否AmazonSecrets Manager 密钥轮换已按照轮换计划成功触发/启动。规则返回 NON_COMPLIANT`RotationOccurringAsScheduled`false。

> Note
>
> 规则将返回 NOT_APPLICABLE。

标识符: SECRETSMANAGER_SCHEDULED_ROTATION_成功_CHECK

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon区域，但亚太地区（雅加达）、亚太地区（大阪）区域除外

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

service-vpc-endpoint-enabled

检查是否已为每个 Amazon VPC 创建规则参数中提供的服务的服务终端节点。如果 Amazon VPC 没有为该服务创建 VPC 终端节点，则该规则将返回 NON_COMPLIANT。

标识符：服务_VPC_ENDPOINT_已启用

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon区域（亚太地区（雅加达）、亚太地区（大阪）区域除外

参数：

serviceName, 类型: 字符串

> 服务的短名称或后缀。注意：要获取可用服务名的列表或有效后缀列表，请使用 DescribeVpcEndpointServices。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

sns-encrypted-kms

检查 Amazon SNS topic 是否使用加密Amazon Key Management Service(AmazonKMS. 如果 Amazon SNS 主题未使用加密，则规则为 NON_COMPLIANTAmazon KMS. 当 `kmsKeyIds` 输入参数中不存在加密 KMS 密钥时，该规则也是 NON_COMPLIANT。

标识符：SNS_ENCRYPTED_KMS

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon区域（亚太地区（大阪）、亚太地区（大阪）、亚太地区（大阪）、

参数：

kmsKeyIds （可选），类型: CSV

以逗号分隔的列表AmazonKMS 密钥 ARN 允许用于加密Amazon SNS 主题。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

ssm-document-not-public

检查是否Amazon账户拥有的Systems Manager 文档是公开的。如果所有者为 Selfpiant 的 SSM 文档是公有的，则规则为 NON_COMPLIANT。

标识符：SSM_DOCUMENT_NOT_PUBLIC

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

vpc-default-security-group-Close

检查任何 Amazon 虚拟私有云 (VPC) 的默认安全组是否不允许入站或出站流量。如果安全组不是默认值，则规则将返回 NOT_APPLICABLE。如果默认安全组具有一个或多个入站或出站流量规则，则规则为 NON_COMPLIANT。

标识符：VPC_DEFAULT_SECURITY_GROUP_已关闭

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon亚太地区（雅加达）区域以外的区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

vpc-flow-logs-enabled

检查是否已为找到并启用Amazon Virtual Private Cloud 流日志。

标识符：VPC_FLOW_LOGS_已启用

触发器类型：定期

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）区域以外的地区

参数：

trafficType（可选），类型: 字符串

TrafficType 流日志

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

vpc-sg-open-only-to-authorized-ports

检查将入站设置为 0.0.0/0 的任何安全组为 TCP 或 UDP 端口。如果将入站设置为 0.0.0/0 的安全组具有规则参数中没有指定的可访问端口，则规则为 NON_COMPLIANT。

标识符：VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

触发器类型：配置更改

Amazon Web Services 区域：全部支持Amazon除亚太地区（雅加达）、亚太地区（大阪）区域以外的区域

参数：

authorizedTcpPorts （可选），类型: 字符串

以逗号分隔，允许向 0.0.0.0/0 开放的 TCP 端口的列表。以短划线定义范围，例如：“443,1020-1025”。

authorizedUdpPorts （可选），类型: 字符串

以逗号分隔，允许向 0.0.0.0/0 开放的 UDP 端口的列表。以短划线定义范围，例如：“500,1020-1025”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。

使用 Amazon Config 托管规则

您可以通过 Amazon Web Services Management Console、Amazon CLI 或 Amazon Config API 设置和激活 Amazon 托管规则。

设置和激活 Amazon 托管规则（控制台）

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在 Amazon Web Services Management Console菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关支持区域的列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
3. 在左侧导航窗格中，选择 Rules。

4. 在 Rules 页面，选择 Add rule。
5. 在 Rules 页面上，可以执行以下操作：
   - 在搜索字段中键入，以便按规则名称、描述和标签筛选结果。例如，键入 EC2 可返回评估 EC2 资源类型的规则，或者键入 periodic 可返回定期触发的规则。
   - 选择箭头图标可查看下一页规则。最近添加的规则标记为 New。
6. 选择要创建的规则。
7. 在 Configure rule 页面，通过完成以下步骤来配置规则：
   a. 对于 Name，请输入一个唯一的规则名称。
   b. 如果规则的触发器类型包括配置更改对于，指定下列选项之一更改范围用哪Amazon Config调用 Lambda 函数：
      - 资源— Resources (资源) 在创建、更改或删除与指定资源类型（或类型和标识符）匹配的资源时。
      - 标签— Resources (标签) 在创建、更改或删除包含指定标签的资源时。
      - 所有更改— 当资源记录的时候Amazon Config已创建、更改或删除。
   c. 如果规则的触发器类型包括定期中，指定Frequency用哪Amazon Config调用 Lambda 函数。
   d. 如果您的规则的 Rule parameters 部分包含参数，则您可以自定义提供的键的值。参数是您的资源为符合规则而必须具备的属性。
8. 选择 Save（保存）。您的新规则将显示在 Rules 页面中。

   合规性将显示评估...。直到Amazon Config有你的规则的评估结果。关于结果的汇总将在几分钟后显示。您可以使用刷新按钮更新结果。

   如果规则或函数没有按预期运行，您可能会在 Compliance 中看到以下一项内容：

   - No results reported (未报告任何结果) - Amazon Config 针对规则评估了您的资源。规则不适用于其范围内的 Amazon 资源，指定的资源已删除，或者评估规则已删除。要获取评估结果，请更新规则、更改其范围或者选择 Re-evaluate。

     如果规则不报告评估结果，该消息可能也会出现。
   - No resources in scope (范围中没有资源) - Amazon Config 无法对照规则来评估您记录的 Amazon 资源，因为您的任何资源都不在规则范围内。要获取评估结果，请编辑规则并更改其范围，或者为Amazon Config使用记录设置页.
   - Evaluations failed (评估失败) - 有关可帮助您确定问题的信息，请选择规则名称以打开其详细信息页面并查看错误消息。

激活 Amazon 托管规则 (Amazon CLI)

使用 `put-config-rule` 命令。

激活 Amazon 托管规则 (API)

使用PutConfigRuleaction.

使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则

对于支持的 Amazon Config 托管规则，您可以使用 Amazon CloudFormation 模板为账户创建规则或更新现有 Amazon CloudFormation 堆栈。堆栈是您作为单个单元配置和更新的相关资源的集合。在使用模板启动堆栈时，将为您创建 Amazon Config 托管规则。模板仅创建规则，而不创建其他 Amazon 资源。

Note

在更新 Amazon Config 托管规则时，将针对最新更改来更新模板。要为规则保存特定版本的模板，请下载该模板并将其上传到您的 S3 存储桶。

有关使用的更多信息Amazon CloudFormation模板，请参阅入门Amazon CloudFormation中的Amazon CloudFormation用户指南.

为 Amazon Config 托管规则启动 Amazon CloudFormation 堆栈

1. 转至 CloudFormation 控制台并创建新堆栈。
2. 对于 Specify template (指定模板)：
   - 如果您已下载模板，请选择 Upload a template file (上传模板文件)，然后选择 Choose file (选择文件) 以上传模板。
   - 还可以选择Amazon S3 URL，然后输入模板 URL`http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template`.

     Note

     规则标识符应该用 ALL_CAPS_WITH_THITH_THINTILES 例如，CLOG_GROUP_GROUP_ENCRYD 而不是云监视日志组加密。
     对于某些规则，规则标识符与规则名称不同。请确保使用规则标识符。例如，受限制的 ssh 的规则标识符是 INCOMINING_SSH_DISABLE。
3. 选择 Next（下一步）。
4. 对于 Specify stack details (指定堆栈详细信息)，键入堆栈名并输入 Amazon Config 规则的参数值。例如，如果您使用的是 `DESIRED_INSTANCE_TYPE` 托管规则模板，则可以指定实例类型，例如“m4.large”。
5. 选择 Next（下一步）。
6. 对于 Options，您可以创建标签或配置其他高级选项。这些操作不是必需的。
7. 选择 Next（下一步）。
8. 对于 Review，验证模板、参数和其他选项是否正确。
9. 选择 Create (创建)。将在几分钟内创建堆栈。您可以在 Amazon Config 控制台中查看创建的规则。

您可以使用模板为 Amazon Config 托管规则创建单个堆栈或更新您的账户中的现有堆栈。如果您删除堆栈，也将删除从该堆栈创建的托管规则。有关更多信息，请参阅 。使用堆栈中的Amazon CloudFormation用户指南.

Amazon Config 自定义规则

您可以使用Guard 自定义策略或 Lambda功能开发自定义策略规则或自定义 Lambda 规则并将其添加到 Amazon Config.

Guard 是 policy-as-code 允许您编写由以下方式强制执行的策略的语言Amazon Config自定义策略规则。使用 Guard 编写的规则可以从Amazon Config使用控制台或Amazon Config规则 API。Amazon Config自定义策略规则允许您创建Amazon Config自定义规则，无需使用 Java 或 Python 来开发 Lambda 函数来管理自定义规则。Amazon Config自定义策略规则是通过配置更改启动的。有关 Guard 的更多信息，请参阅Data GitHub 存储库.

自定义 Lambda 规则为您提供了使用 Java 或 Python 为Amazon Config自定义规则。一个Lambda 函数是你上传到的自定义代码Amazon Lambda，由事件源发布给它的事件调用。如果 Lambda 函数与Amazon

Config规则，Amazon Config在规则启动时调用它。之后，Lambda 函数会评估由发送的配置信息。Amazon Config，然后返回评估结果。有关 Lambda 函数的更多信息，请参阅功能和事件来源中的Amazon Lambda 开发人员指南.

主题

创建Amazon Config自定义策略规则

你可以创建Amazon Config来自的自定义策略规则Amazon Web Services Management Console、Amazon CLI，或者Amazon ConfigAPI。有关如何使用 Guard 编写规则的更多信息，请参阅编写 Guard 规则中的 Amazon CloudFormationGuard 用户指南。有关受支持资源类型模式的更多信息，请参阅以下内容Amazon Config可以评估，请参阅资源类型中的Amazon Config资源架构 GitHub 存储库。

创建Amazon Config自定义策略规则（控制台）

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在Amazon Web Services Management Console菜单上，验证区域选择器是否设置为Amazon支持的区域Amazon Config规则。有关支持的区域列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
3. 在左侧导航窗格中，选择 Rules。
4. 在 Rules 页面，选择 Add rule。
5. 在存储库的指定规则类型页面上，选择使用 Guard 创建自定义规则.
6. 在存储库的配置规则页面上，请完成以下步骤来创建规则：

   a. 适用于规则名称，键入唯一的规则名称。

   b. 适用于说明，键入规则的说明。

   c. 适用于Guard 运行时版本中，为你的选择运行时系统Amazon Config自定义策略规则。

   d. 适用于规则内容，您可以使用规则的 Guard Custom 策略填充它。有关 Guard 自定义策略的结构和功能的更多信息，请参阅Amazon CloudFormationGuard 2.0 的操作模式在警卫队 GitHub 存储库。

      以下示例显示的策略定义：Amazon Config的自定义策略规则版本Amazon Config托管规则dynamodb-pitr-enabled (p. 139)

```
# This rule checks if point in time recovery (PITR) is enabled on active Amazon
 DynamoDB tables
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
        let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
        %pitr == "ENABLED"
}
```

   e. 适用于触发器、Amazon Config自定义策略规则由配置更改. 此选项将被预先选择。

指定以下选项之一：更改的范围：

- 资源— Resource (资源) 在创建、更改或删除与指定资源类型（或类型和标识符）匹配的资源时。
- 标签— Tags (标签) 在创建、更改或删除包含指定标签的资源时。
- 所有更改— 当资源记录的时候Amazon Config已创建、更改或删除。

f. 如果你的规则包括参数，请在规则参数部分您可以自定义提供的键的值。参数是您的资源为符合规则而必须具备的属性。

7. 编辑完规则后，选择下一步. 在存储库的审核和创建页面，您可以在将规则添加到Amazonaccount.
8. 当你完成规则审查后，选择添加规则.

创建Amazon Config自定义策略规则 (Amazon CLI)

使用 `put-config-rule` 命令。

这些区域有：`Owner`字段应该是`CUSTOM_POLICY`. 以下附加字段是必填字段。Amazon Config自定义策略规则：

- `Runtime`: 你的运行时系统Amazon Config自定义策略规则。
- `PolicyText`：包含您的逻辑的策略定义Amazon Config自定义策略规则。
- `EnableDebugLogDelivery`：用于为你的启用调试日志记录的布尔表达式Amazon Config自定义策略规则。原设定值为 `false`。

创建Amazon Config自定义策略规则 (API)

使用PutConfigRuleaction.

这些区域有：`Owner`字段应该是`CUSTOM_POLICY`. 以下附加字段是必填字段。Amazon Config自定义策略规则：

- `Runtime`: 你的运行时系统Amazon Config自定义策略规则。
- `PolicyText`：定义你的逻辑的策略Amazon Config自定义策略规则。
- `EnableDebugLogDelivery`：用于为你的启用调试日志记录的布尔表达式Amazon Config自定义策略规则。原设定值为 `false`。

创建Amazon Config自定义 Lambda 规则

您可以编写自定义规则并将其添加至Amazon Config和Amazon Lambda函数。您可以将每个自定义规则与一个 Lambda 函数关联，其中包含用于评估您的Amazon资源符合该规则。将此函数与您的规则关联后，该规则会定期或因响应配置更改而调用该函数。然后，该函数评估您的资源是否符合您的规则，并将评估结果发送给 Amazon Config。

中的示例自定义 Lambda 规则（Amazon EC2 示例）(p. 186)指导您完成首次创建自定义 Lambda 规则，该规则评估您的每个 EC2 实例是否为 t2.micro 类型。其中包含可以添加至的示例 Lambda 函数Amazon Lambda没有修改。中的示例自定义 Lambda 规则（一般示例）(p. 188)提供了创建自定义 Lambda 规则的一般示例。

要了解如何操作Amazon Lambda函数的工作原理以及如何编写此函数，请参阅Amazon Lambda开发人员指南.

主题

自定义 Lambda 规则（Amazon EC2 示例）

此过程将指导您完成创建自定义 Lambda 规则的过程，该规则评估您的每个 EC2 实例是否为 t2.micro 类型。Amazon Config将针对此规则运行基于事件的评估，这意味着它将每次检查您的实例配置Amazon Config检测实例中的配置更改。Amazon Config将 t2.micro 实例标记为合规，所有其他实例都标记为不合规。合规性状态将显示在 Amazon Config 控制台中。

为保证这一程序的最佳效果，您的 Amazon 账户应该拥有一个或多个 EC2 实例。您的实例中应包含至少一个 t2.micro 实例和其他类型的实例。

要创建此规则，请先通过在 Amazon Lambda 控制台中自定义一个蓝图来创建一个 Amazon Lambda 函数。然后，您将在中创建自定义 Lambda 规则Amazon Config，您将将使用规则与函数相关联。

主题

为自定义 Config 规则创建 Amazon Lambda 函数

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Lambda 控制台：https://console.aws.amazon.com/lambda/。
2. 在 Amazon Web Services Management Console菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关支持的区域的列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
3. 在Amazon Lambda选择控制台、创建 Lambda 函数.
4. 选择 Use a blueprint (使用蓝图)。在搜索栏中，键入触发配置规则更改. 在筛选结果中选择蓝图并选择配置.
5. 在 Configure triggers 页面上，选择 Next。
6. 在基本信息页面上，完成以下步骤：
   a. 对于函数名称，请键入 **`InstanceTypeCheck`**。
   b. 适用于执行角色，选择从创建新角色AmazonPolicy templates.
   c. 对于 Runtime，请保留 Node.js。
   d. 适用于Role name (角色名称)，键入名称。
   e. 适用于Policy templates，选择Amazon Config规则权限.
   f. 适用于Lambda 函数代码函数中，保留预配置的代码。代码编辑器中带有用于您的函数的 Node.js 代码。在本程序中，您无需更改代码。
   g. 验证详细信息并选择创建函数. Amazon Lambda 控制台会显示您的函数。
7. 要验证您的函数是否设置正确，请通过以下步骤进行测试：
   a. 选择测试从下面的菜单中选择函数概述然后选择，配置测试事件.
   b. 适用于模板，选择Amazon Config配置项变更通知.
   c. 对于 Name (名称)，键入名称。
   d. 选择测试.Amazon Lambda使用示例事件来测试您的函数。如果您的函数按预期运行，Execution result 下会出现与下面类似的错误消息：

```
{
```

```
  "errorType": "InvalidResultTokenException,"
  "errorMessage": "Result Token provided is invalid",
. . .
```

此处预期为 `InvalidResultTokenException`，因为仅当您的函数从 收到结果令牌Amazon Config 时，它才能成功运行。结果令牌可以识别 Amazon Config 规则和引起评估的事件，并将评估与规则相关联。这一异常表示您的函数具备将结果发送至 Amazon Config 所需的权限。否则，将出现以下错误消息：`not authorized to perform: config:PutEvaluations`. 如果发生这一错误，请更新您分配给函数的角色，以便允许`config:PutEvaluations`操作，然后再次测试您的函数。

创建自定义 Lambda 规则以评估 Amazon EC2 实例

1. 通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在Amazon Web Services Management Console菜单中，验证区域选择器中的区域是否与您创建Amazon Lambda适用于自定义 Lambda 规则的函数。
3. 在 Rules 页面，选择 Add rule。
4. 在存储库的指定规则类型选择页面，选择创建自定义规则.
5. 在 Configure rule 页面，完成以下步骤：

   a. 对于名称，键入 **`InstanceTypesAreT2micro`**。
   b. 对于描述，键入 **`Evaluates whether EC2 instances are the t2.micro type`**。
   c. 适用于Amazon Lambda函数 ARN，指定 ARNAmazon Lambda分配给你的函数。

      Note

      您在此步骤中指定的 ARN 不能包含 `$LATEST` 限定词。您指定的 ARN 可以不带有版本限定词，也可以带有除 `$LATEST` 之外的任何限定词。Amazon Lambda 支持函数版本控制功能，并为每个版本都分配一个带有限定词的 ARN。Amazon Lambda 对最新版本使用 `$LATEST` 限定词。

   d. 适用于触发器类型，选择配置发生更改时.
   e. 对于 Scope of changes，请选择 Resources。
   f. 适用于资源，选择AmazonEC2 实例来自 的资源类型下拉列表。
   g. 在参数部分中，您必须指定您的规则参数Amazon Lambda函数评估并获得所需的值。本程序中的函数会评估 `desiredInstanceType` 参数。

      对于 Key (键)，键入 **`desiredInstanceType`**。对于 Value，键入 **`t2.micro`**。
6. 选择 Next（下一步）。在存储库的审核和创建页面，验证您的规则的详细信息，然后选择添加规则函数. 您的新规则将显示在Rule页.

   合规性将显示评估...。直到Amazon Config接收来自您的评估结果Amazon Lambdafunction. 如果规则和函数按预期运行，关于结果的汇总将在几分钟后显示。例如，2 noncompliant resource(s) 结果表示您的实例中有两个不是 t2.micro 实例，Compliant 结果表示所有实例均为 t2.micro 实例。您可以使用刷新按钮更新结果。

   如果规则或函数没有按预期运行，您可能会在 Compliance 中看到以下一项内容：

   - No results reported (未报告任何结果) - Amazon Config 针对规则评估了您的资源。规则不适用于其范围内的 Amazon 资源，指定的资源已删除，或者评估规则已删除。要获取评估结果，请更新规则、更改其范围或者选择 Re-evaluate。

     验证范围是否包括AmazonEC2 实例为了资源，然后重试。
   - No resources in scope (范围中没有资源) - Amazon Config 无法对照规则来评估您记录的 Amazon 资源，因为您的任何资源都不在规则范围内。要获取评估结果，请编辑规则并更改其范围或添加资源Amazon Config使用录制设置页.

请检查确认 Amazon Config 是否在记录 EC2 实例。

- Evaluations failed (评估失败) - 有关可帮助您确定问题的信息，请选择规则名称以打开其详细信息页面并查看错误消息。

如果您的规则正常运行并且 Amazon Config 提供了评估结果，您可以了解哪些条件影响了规则的合规性状态。您可以了解哪些资源不合规 (如果有) 及其原因。有关更多信息，请参阅查看配置合规性 (p. 63)。

自定义 Lambda 规则（一般示例）

完成以下过程以创建自定义 Lambda 规则。要创建自定义 Lambda 规则，您首先创建Amazon Lambda 函数，其中包含该规则的评估逻辑。然后，您将该函数与您在创建的自定义 Lambda 规则关联。Amazon Config.

Important

作为允许的最佳安全实践Amazon Config调用 Lambda 函数的权限，我们强烈建议您在基于资源的策略中限制 Lambda 的访问`sourceARN`和/或`sourceAccountId`在调用请求中。有关更多信息，请参阅 的安全最佳实践Amazon Lambda基于资源的策略 (p. 190)。

目录

为自定义 Config 规则创建 Amazon Lambda 函数

一个Lambda 函数是你上传到的自定义代码Amazon Lambda，并且由事件源发布给它的事件调用。如果 Lambda 函数与 Config 规则关联，Amazon Config在触发规则时调用它。然后，Lambda 函数将评估由发送的配置信息。Amazon Config，然后返回评估结果。有关 Lambda 函数的更多信息，请参阅功能和事件来源中的Amazon Lambda开发人员指南.

您可以使用支持的编程语言Amazon Lambda为自定义 Lambda 规则创建 Lambda 函数。为简化这一任务，您可以自定义Amazon Lambda蓝图或重复使用Amazon ConfigRule GitHub 存储库。

Amazon Lambda 蓝图

Amazon Lambda 控制台可以提供示例函数或蓝图，您可以通过添加自己的评估逻辑来对其进行自定义。当您创建函数时，您可以选择以下蓝图之一：

- 触发配置规则更改— 在您的时触发Amazon资源配置更改。
- 配置规则-周期性— 按照您选择的频率（例如，每 24 小时）触发。

Amazon ConfigRule GitHub 知识库

自定义 Lambda 规则示例函数的公开存储库，GitHub 是一项基于网络的代码托管和共享服务。示例函数由 Amazon 社区开发和提供。如果想使用示例函数，您可以将其代码复制到新的 Amazon Lambda 函数中。要查看存储库，请访问 https://github.com/awslabs/aws-config-rules/。

为您的自定义规则创建函数

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Lambda 控制台：https://console.aws.amazon.com/lambda/。

2. 在 Amazon Web Services Management Console菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关支持区域的列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
3. 选择 Create a Lambda function (创建 Lambda 函数)。
4. 在存储库的使用蓝图页面上，您可以为Amazon Config将规则作为起点，或者您可以通过选择不使用蓝图继续操作跳过.
5. 在 Configure triggers 页面上，选择 Next。
6. 在存储库的基本信息页面上，键入一个名称和描述。
7. 对于 Runtime，请选择您编写函数时使用的编程语言。
8. 对于 Code entry type，请选择您偏好的条目类型。如果您正在使用蓝图，请保留预配置的代码。
9. 用您选择的代码条目类型要求的方法提供您的代码。如果您正在使用蓝图，那么函数代码由代码编辑器提供，且您可以自定义代码，以使其包含您自己的评估逻辑。当 Amazon Config 调用您的函数时，您的代码可以评估它提供的事件数据：

   - 对于基于 config-rule-change-triggered 蓝图的函数或由配置更改触发的函数，事件数据是更改的 Amazon 资源的配置项或过大配置项对象。
   - 对于基于 config-rule-periodic 蓝图的函数，或按照您选择的频率触发的函数，事件数据是一个 JSON 对象，包括有关评估触发时间的信息。
   - 对于这两种类型的函数，Amazon Config 会传递 JSON 格式的规则参数。您在中创建自定义 Lambda 规则时，您可以定义传递哪个规则参数。Amazon Config.
   - 有关 Amazon Config 在调用您的函数时发布的事件示例，请参阅 Amazon Config 规则的示例事件 (p. 202)。
10. 适用于执行角色，选择从创建新角色AmazonPolicy templates.
11. 对于 Role name，请输入名称。
12. 适用于Policy templates，选择AmazonConfig rules 权限.
13. 验证详细信息并选择创建函数.

在 Amazon Config 中创建自定义规则

使用Amazon Config将创建自定义 Lambda 规则并将其与 Lambda 函数关联。

创建自定义规则

1. 通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在Amazon Web Services Management Console菜单中，验证区域选择器中的区域是否与您创建 Amazon Lambda适用于自定义 Lambda 规则的函数。
3. 在 Rules 页面，选择 Add rule。
4. 在存储库的指定规则类型页面，选择创建自定义规则.
5. 在 Configure rule 页面，键入一个名称和描述。
6. 适用于Amazon Lambda函数 ARN对于，指定 ARNAmazon Lambda分配给你的函数。

   Note

   您在此步骤中指定的 ARN 不能包含 `$LATEST` 限定词。您指定的 ARN 可以不带有版本限定词，也可以带有除 `$LATEST` 之外的任何限定词。Amazon Lambda 支持函数版本控制功能，并为每个版本都分配一个带有限定词的 ARN。Amazon Lambda 对最新版本使用 `$LATEST` 限定词。
7. 对于 Trigger type，请选择下列一个或两个选项：

   - 配置更改–Amazon Config在检测到配置更改时调用 Lambda 函数。

- 定期–Amazon Config按照您选择的频率（例如，每 24 小时）调用您的 Lambda 数。

8. 如果规则的触发器类型包括配置更改对于，指定下列选项之一更改范围用哪Amazon Config调用 Lambda 函数：
   - 所有更改— 何时记录的任何资源Amazon Config已创建、更改或删除。
   - 资源— Resource (类型和标识符) 匹配的资源被创建、更改或删除时。
   - 标签— 在创建、更改或删除包含指定标签的任何资源时
9. 如果规则的触发器类型包括定期中，指定Frequency用哪Amazon Config调用 Lambda 函数。
10. 在参数部分中，指定任何规则参数Amazon Lambda函数评估并获得所需的值。
11. 选择 Next（下一步）。在存储库的审核和创建页面，验证有关您的规则的详细信息，然后选择添加规则函数. 您的新规则将显示在Rule页.

    合规性将显示正在评估...直到Amazon Config接收来自您的评估结果Amazon Lambdafunction. 如果规则和函数按预期运行，结果汇总将在几分钟后显示。您可以使用刷新按钮更新结果。

    如果规则或函数没有按预期运行，您可能会在 Compliance 中看到以下一项内容：

    - No results reported (未报告任何结果) - Amazon Config 针对规则评估了您的资源。规则不适用于其范围内的 Amazon 资源，指定的资源已删除，或者评估规则已删除。要获取评估结果，请更新规则、更改其范围或者选择 Re-evaluate。

      如果规则不报告评估结果，该消息可能也会出现。
    - No resources in scope (范围中没有资源) - Amazon Config 无法对照规则来评估您记录的 Amazon 资源，因为您的任何资源都不在规则范围内。您可以选择哪些资源Amazon Config记录设置页.
    - Evaluations failed (评估失败) - 有关可帮助您确定问题的信息，请选择规则名称以打开其详细信息页面并查看错误消息。

    Note

    当您使用Amazon ConfigConsole (控制台)，系统将自动为您创建适当权限。如果 Lambda 使用Amazon CLI，你需要给Amazon ConfigLambda 用`aws lambda add-permission`命令。有关更多信息，请参阅 。对 使用基于资源的策略Amazon Lambda（Lambda 函数策略）中的Amazon Lambda开发人员指南.
    在给予之前Amazon Config调用 Lambda 函数的权限，请参阅以下部分的安全最佳实践Amazon Lambda基于资源的策略 (p. 190).

的安全最佳实践Amazon Lambda基于资源的策略

作为安全最佳实践，为避免对整个服务主体名称 (SPN) 授予调用权限以调用 Lambda 函数，我们强烈建议您在基于 Lambda 资源的策略中限制访问`sourceARN`和/或`sourceAccountId`在调用请求中。

这些区域有：`sourceARN`ARN 是Amazon Config调用 Lambda 函数的规则。

这些区域有：`sourceAccountId`是创建规则的用户的账户 ID。

在基于 Lambda 资源的策略中限制访问权限有助于确保Amazon Lambda仅代表预期的用户和场景访问您的资源。

要添加基于 SPN 的权限，您需要使用以下 CLI

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com
```

添加 SourceAccountId 基于权限

在创建规则之前，您可以添加`sourceAccountId`使用以下 CLI 访问基于资源的策略的权限

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID
```

添加这两者的 SourceArn 和 SourceAccountId 基于权限

创建规则后，您可以添加`sourceARN`使用以下 CLI 授予基于资源的策略的权限。这仅允许特定规则 ARN 调用 Lambda 函数。

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID --source-arn ARN of the created config rule
```

评估其他资源类型

您可以创建自定义 Lambda 规则来针对不记录的资源类型运行评估。Amazon Config. 如果要评估以下资源类型的合规性，这会很有用：Amazon Config目前没有记录。有关您可以使用自定义 Lambda 规则评估的其他资源类型的列表，请参阅Amazon资源类型参考.

> **Note**
>
> 列表Amazon CloudFormation《用户指南》可能包含最近添加，但尚不可用于在中创建自定义 Lambda 规则的资源类型。Amazon Config.Amazon Config定期添加资源类型支持。

示例

1. 您想评估账户中的 Amazon S3 Glacier 保险库。目前未记录 Amazon S3 Glacier 文件库资源Amazon Config.
2. 你创建Amazon Lambda函数，以评估您的 Amazon S3 Glacier 文件库是否符合您的账户要求。
3. 您创建了名为的自定义 Lambda 规则评估冰川-金库然后分配你的Amazon Lambda适用于规则的函数。
4. Amazon Config将调用您的 Lambda 函数，然后按照您的规则评估 Amazon S3 Glacier 文件库。
5. Amazon Config 返回评估结果，您可以查看您的规则的合规性结果。

> **Note**
>
> 您可以查看 Amazon Config 时间线中的配置详细信息，并在 Amazon Config 支持的资源的 Amazon Config 控制台中查找资源。如果您配置 Amazon Config 以记录所有资源类型，则新添加的支持资源将被自动记录。有关更多信息，请参阅支持的资源类型 (p. 7)。

针对 Amazon Config 规则的 Amazon Lambda 函数和事件示例

每个自定义 Lambda 规则都与 Lambda 关联功能，其中包含规则评估逻辑的自定义代码。发生 Config 规则的触发器时（例如，当Amazon Config检测到配置更改），Amazon Config通过发布一个来调用规则的 Lambda 函数事件，它是一个 JSON 对象，用于提供函数评估的配置数据。

有关函数和事件的更多信息，请参阅Amazon Lambda请参阅功能和事件来源中的Amazon Lambda开发人员指南.

主题

- Amazon Config 规则的示例事件 (p. 202)

用于 Amazon Config 规则 (Node.js) 的示例 Amazon Lambda 函数

Amazon Lambda 将执行函数来响应由 Amazon 服务发布的事件。的函数Amazon Config自定义 Lambda 规则接收由发布的事件Amazon Config，然后该函数使用它从事件接收以及它从Amazon Config用于评估规则的合规性的 API。用于 Config 规则的函数的运作方式会因其执行的评估是由配置更改触发还是定期触发而有所不同。

有关通用模式的信息Amazon Lambda函数，请参阅编程模型中的Amazon Lambda开发人员指南.

目录

评估由配置更改触发时的示例函数

Amazon Config 检测到自定义规则范围内的资源发生配置更改时，会调用函数示例如下。

如果您使用 Amazon Config 控制台创建与类似此示例的函数关联的规则，请选择 Configuration changes (配置更改) 作为触发器类型。如果您使用 Amazon Config API 或 Amazon CLI 创建规则，请将 `MessageType` 属性设置为 `ConfigurationItemChangeNotification` 和 `OversizedConfigurationItemChangeNotification`。这些设置可使您的规则在每次 Amazon Config 生成配置项或资源更改导致过大配置项时触发。

此示例评估您的资源并检查实例是否匹配资源类型 `AWS::EC2::Instance`。此规则在 Amazon Config 生成配置项或过大配置项通知时触发。

```
'use strict';

const aws = require('aws-sdk');

const config = new aws.ConfigService();


// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}

// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory API.
function getConfiguration(resourceType, resourceId, configurationCaptureTime, callback) {
    config.getResourceConfigHistory({ resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 }, (err, data) => {
        if (err) {
            callback(err, null);
        }
        const configurationItem = data.configurationItems[0];
        callback(null, configurationItem);
    });
}
```

```
// Convert the oversized configuration item from the API model to the original invocation
 model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash = apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the configurationItem
 object in the invoking event or with the getResourceConfigHistory API in the
 getConfiguration function.
function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
       const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem) => {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
       });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope ===
 false;
}

// In this example, the resource is compliant if it is an instance and its type matches the
 type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration, 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
        return 'COMPLIANT';
    }
```

```
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
exports.handler = (event, context, callback) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    getConfigurationItem(invokingEvent, (err, configurationItem) => {
        if (err) {
            callback(err);
        }
        let compliance = 'NOT_APPLICABLE';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
        }
        // Initializes the request that contains the evaluation results.
        putEvaluationsRequest.Evaluations = [
            {
                ComplianceResourceType: configurationItem.resourceType,
                ComplianceResourceId: configurationItem.resourceId,
                ComplianceType: compliance,
                OrderingTimestamp: configurationItem.configurationItemCaptureTime,
            },
        ];
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        config.putEvaluations(putEvaluationsRequest, (error, data) => {
            if (error) {
                callback(error, null);
            } else if (data.FailedEvaluations.length > 0) {
                // Ends the function if evaluation results are not successfully reported to
 AWS Config.
                callback(JSON.stringify(data), null);
            } else {
                callback(null, data);
            }
        });
    });
};
```

函数运作

本函数在运行时执行以下操作：

1. 该函数运行时Amazon Lambda传递`event`对象执行`handler`function. 在本示例中，函数接受可选的`callback`参数，用于向发起人返回消息。Amazon Lambda还可以通过`context`对象，其中包含此函数在运行时可以使用的信息和方法。请注意，在较新版本的 Lambda 中，不再使用上下文。
2. 此函数检查事件的 `messageType` 是配置项还是过大配置项，然后返回配置项。
3. 处理程序调用 `isApplicable` 函数来确定资源是否已删除。
4. 处理程序调用 `evaluateChangeNotificationCompliance` 函数并传递 Amazon Config 在事件中发布的 `configurationItem` 和 `ruleParameters` 对象。

   函数首先评估资源是否为 EC2 实例。如果资源不是 EC2 实例，函数会返回 `NOT_APPLICABLE` 这一合规性值。

   然后，函数评估配置项中的 `instanceType` 属性是否与 `desiredInstanceType` 参数值一致。如果值相等，该函数将返回 `COMPLIANT`。如果值不相等，该函数将返回 `NON_COMPLIANT`。

5. 处理程序通过初始化 `putEvaluationsRequest` 对象来做好向 Amazon Config 发送评估结果的准备。该对象包含 `Evaluations` 参数，这一参数用于识别受评估资源的合规性结果、资源类型和 ID。`putEvaluationsRequest` 对象还包含来自事件的结果令牌，该令牌可标识 Amazon Config 的规则和事件。
6. 处理程序通过向 `config` 客户端的 `putEvaluations` 方法传递对象来向 Amazon Config 发送评估结果。

定期评估时的示例函数

Amazon Config 针对定期评估调用的函数示例如下。定期评估按您在 Amazon Config 中定义规则时指定的频率进行。

如果您使用 Amazon Config 控制台创建与类似此示例的函数关联的规则，请选择 Periodic (定期) 作为触发器类型。如果您使用 Amazon Config API 或 Amazon CLI 创建规则，请将 `MessageType` 属性设置为 `ScheduledNotification`。

本示例会检查指定资源的总数是否超出指定的最大值。

```
var aws = require('aws-sdk'), // Loads the AWS SDK for JavaScript.
    config = new aws.ConfigService(), // Constructs a service object to use the
 aws.ConfigService class.
    COMPLIANCE_STATES = {
        COMPLIANT : 'COMPLIANT',
        NON_COMPLIANT : 'NON_COMPLIANT',
        NOT_APPLICABLE : 'NOT_APPLICABLE'
    };

// Receives the event and context from AWS Lambda.
exports.handler = function(event, context, callback) {
    // Parses the invokingEvent and ruleParameters values, which contain JSON objects
 passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        noOfResources = 0;

    if (isScheduledNotification(invokingEvent)) {
        countResourceTypes(ruleParameters.applicableResourceType, "", noOfResources,
 function(err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                // Initializes the request that contains the evaluation results.
                putEvaluationsRequest = {
                    Evaluations : [ {
                        // Applies the evaluation result to the AWS account published in
 the event.
                        ComplianceResourceType : 'AWS::::Account',
                        ComplianceResourceId : event.accountId,
                        ComplianceType : evaluateCompliance(ruleParameters.maxCount,
 count),
                        OrderingTimestamp : new Date()
                    } ],
                    ResultToken : event.resultToken
                };
                // Sends the evaluation results to AWS Config.
                config.putEvaluations(putEvaluationsRequest, function(err, data) {
                    if (err) {
                        callback(err, null);
                    } else {
                        if (data.FailedEvaluations.length > 0) {
                            // Ends the function execution if evaluation results are not
 successfully reported
                            callback(JSON.stringify(data));
```

```
                        }
                        callback(null, data);
                    }
                });
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return COMPLIANCE_STATES.NON_COMPLIANT;
    } else {
        return COMPLIANCE_STATES.COMPLIANT;
    }
}

// Counts the applicable resources that belong to the AWS account.
function countResourceTypes(applicableResourceType, nextToken, count, callback) {
    config.listDiscoveredResources({resourceType : applicableResourceType, nextToken :
 nextToken}, function(err, data) {
        if (err) {
            callback(err, null);
        } else {
            count = count + data.resourceIdentifiers.length;
            if (data.nextToken !== undefined && data.nextToken != null) {
                countResourceTypes(applicableResourceType, data.nextToken, count,
 callback);
            }
            callback(null, count);
        }
    });
    return count;
}
```

函数运作

本函数在运行时执行以下操作：

1. 该函数运行时Amazon Lambda传递`event`对象执行`handler`function. 在本示例中，函数接受可选的`callback`参数，用于向发起人返回消息。Amazon Lambda还可以通过`context`对象，其中包含此函数在运行时可以使用的信息和方法。请注意，在较新版本的 Lambda 中，不再使用上下文。
2. 为计数指定类型的资源，处理程序会调用 `countResourceTypes` 函数，而且它传递其从事件收到的 `applicableResourceType` 参数。`countResourceTypes` 函数调用 `listDiscoveredResources` 客户端的 `config` 方法，该方法返回适用资源的标识符列表。该函数使用此列表的长度来确定适用资源的数量，而且它将此计数返回到处理程序。
3. 处理程序通过初始化 `putEvaluationsRequest` 对象来做好向 Amazon Config 发送评估结果的准备。此对象包括`Evaluations`参数，用于标识合规性结果和Amazon Web Services 账户这是在活动中公布的。您可以使用 `Evaluations` 参数将结果应用于 Amazon Config 支持的任何资源类型。`putEvaluationsRequest` 对象还包含来自事件的结果令牌，该令牌可标识 Amazon Config 的规则和事件。

4. 在 `putEvaluationsRequest` 对象中，处理程序调用 `evaluateCompliance` 函数。此函数测试适用资源的数量是否超出分配给事件所提供的 `maxCount` 参数的最大值。如果资源的数量超出最大值，函数将返回 `NON_COMPLIANT`。如果资源的数量没有超出最大值，函数将返回 `COMPLIANT`。
5. 处理程序通过向 `config` 客户端的 `putEvaluations` 方法传递对象来向 Amazon Config 发送评估结果。

示例Amazon Lambda用于的函数Amazon Config规则 (Python)

Amazon Lambda 将执行函数来响应由 Amazon 服务发布的事件。的函数Amazon Config自定义 Lambda 规则接收由发布的事件Amazon Config然后该函数使用它从事件接收以及它从Amazon Config用于评估规则的合规性的 API。用于 Config 规则的函数的运作方式会因其执行的评估是由配置更改触发还是定期触发而有所不同。

有关其中的通用模式的信息Amazon Lambda函数，请参阅编程模型中的Amazon Lambda开发人员指南.

目录

评估由配置更改触发时的示例函数

Amazon Config 检测到自定义规则范围内的资源发生配置更改时，会调用函数示例如下。

如果您使用 Amazon Config 控制台创建与类似此示例的函数关联的规则，请选择 Configuration changes (配置更改) 作为触发器类型。如果您使用 Amazon Config API 或 Amazon CLI 创建规则，请将 `MessageType` 属性设置为 `ConfigurationItemChangeNotification` 和 `OversizedConfigurationItemChangeNotification`。这些设置可使您的规则在每次 Amazon Config 生成配置项或资源更改导致过大配置项时触发。

```
import boto3
import json

# Set to True to get the lambda to assume the Role attached on the Config Service (useful
 for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling the
 client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
```

```
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] = json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary = check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
```

```
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'], 'configuration_item[\'configuration
\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

函数运作

本函数在运行时执行以下操作：

1. 该函数运行时Amazon Lambda传递`event`对象执行`handler`function. 在本示例中，函数接受可选的`callback`参数，用于向发起人返回消息。Amazon Lambda还可以通过`context`对象，其中包含此函数在运行时可以使用的信息和方法。请注意，在较新版本的 Lambda 中，不再使用上下文。
2. 此函数检查事件的 `messageType` 是配置项还是过大配置项，然后返回配置项。

3. 处理程序调用 `isApplicable` 函数来确定资源是否已删除。
4. 处理程序调用 `evaluateChangeNotificationCompliance` 函数并传递 Amazon Config 在事件中发布的 `configurationItem` 和 `ruleParameters` 对象。

   函数首先评估资源是否为 EC2 实例。如果资源不是 EC2 实例，函数会返回 `NOT_APPLICABLE` 这一合规性值。

   然后，函数评估配置项中的 `instanceType` 属性是否与 `desiredInstanceType` 参数值一致。如果值相等，该函数将返回 `COMPLIANT`。如果值不相等，该函数将返回 `NON_COMPLIANT`。
5. 处理程序通过初始化 `putEvaluationsRequest` 对象来做好向 Amazon Config 发送评估结果的准备。该对象包含 `Evaluations` 参数，这一参数用于识别受评估资源的合规性结果、资源类型和 ID。`putEvaluationsRequest` 对象还包含来自事件的结果令牌，该令牌可标识 Amazon Config 的规则和事件。
6. 处理程序通过向 `config` 客户端的 `putEvaluations` 方法传递对象来向 Amazon Config 发送评估结果。

定期评估时的示例函数

Amazon Config 针对定期评估调用的函数示例如下。定期评估按您在 Amazon Config 中定义规则时指定的频率进行。

如果您使用 Amazon Config 控制台创建与类似此示例的函数关联的规则，请选择 Periodic (定期) 作为触发器类型。如果您使用 Amazon Config API 或 Amazon CLI 创建规则，请将 `MessageType` 属性设置为 `ScheduledNotification`。

```
import boto3
import json

# Set to True to get the lambda to assume the Role attached on the Config Service (useful
 for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling the
 client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
```

```
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value to the
 handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report on the
 rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    valid_rule_parameters = evaluate_parameters(rule_parameters)
```

```
    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
count_resource_types(valid_rule_parameters['applicableResourceType'], '', resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
ResultToken=event['resultToken'])
```

函数运作

本函数在运行时执行以下操作：

1. 该函数运行时Amazon Lambda传递`event`对象执行`handler`function. 在本示例中，函数接受可选的`callback`参数，用于向发起人返回消息。Amazon Lambda还可以通过`context`对象，其中包含此函数在运行时可以使用的信息和方法。请注意，在较新版本的 Lambda 中，不再使用上下文。
2. 为计数指定类型的资源，处理程序会调用 `countResourceTypes` 函数，而且它传递其从事件收到的 `applicableResourceType` 参数。`countResourceTypes` 函数调用 `listDiscoveredResources` 客户端的 `config` 方法，该方法返回适用资源的标识符列表。该函数使用此列表的长度来确定适用资源的数量，而且它将此计数返回到处理程序。
3. 处理程序通过初始化 `putEvaluationsRequest` 对象来做好向 Amazon Config 发送评估结果的准备。此对象包括`Evaluations`参数，用于标识合规性结果和Amazon Web Services 账户这是在活动中公布的。您可以使用 `Evaluations` 参数将结果应用于 Amazon Config 支持的任何资源类型。`putEvaluationsRequest` 对象还包含来自事件的结果令牌，该令牌可标识 Amazon Config 的规则和事件。
4. 在 `putEvaluationsRequest` 对象中，处理程序调用 `evaluateCompliance` 函数。此函数测试适用资源的数量是否超出分配给事件所提供的 `maxCount` 参数的最大值。如果资源的数量超出最大值，函数将返回 `NON_COMPLIANT`。如果资源的数量没有超出最大值，函数将返回 `COMPLIANT`。
5. 处理程序通过向 `config` 客户端的 `putEvaluations` 方法传递对象来向 Amazon Config 发送评估结果。

Amazon Config 规则的示例事件

当触发规则时，Amazon Config 会通过发布一个事件来调用该规则的 Amazon Lambda 函数。然后，Amazon Lambda 会将事件传递到该函数的处理程序，从而执行该函数。

由配置更改触发的评估的示例事件

当 Amazon Config 检测到规则范围内的资源的配置更改时，它会发布一个事件。下面的示例事件演示规则被某个 EC2 实例的配置更改所触发。

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime\":
\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",\"configurationItemStatus\":
\"OK\",\"resourceId\":\"i-00000000\",\"ARN\":\"arn:aws:ec2:us-east-2:123456789012:instance/
i-00000000\",\"awsRegion\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",
\"resourceType\":\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":
[{\"resourceId\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":
\"Is attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
```

```
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

由过大配置更改触发的评估的示例事件

某些资源更改会生成过大配置项。下面的示例事件演示规则被某个 EC2 实例的过大配置更改所触发。

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\": \"UPDATE
\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime\":
\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\": \"OK\",\"resourceType\": \"AWS::EC2::Instance\",
\"resourceId\":\"i-00000000\",\"resourceName\":null,\"ARN\":\"arn:aws:ec2:us-
west-2:123456789012:instance/i-00000000\",\"awsRegion\": \"us-west-2\",\"availabilityZone
\":\"us-west-2a\",\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-rule-
ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

由定期频率触发的评估的示例事件

当 Amazon Config 以您指定的频率 (如每 24 小时) 评估您的资源时，它会发布一个事件。下面的示例事件演示规则被定期频率触发。

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime\":
\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",\"recordVersion\":
\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

事件属性

Amazon Config 事件的 JSON 对象包含以下属性：

`invokingEvent`

触发规则评估的事件。如果事件是为了响应资源配置更改而发布的，则此属性的值是一个包含 JSON `configurationItem` 或 `configurationItemSummary` (对于过大配置项) 的字符串。该配置项表示相关资源在 Amazon Config 检测到更改时的状态。有关配置项的示例，请参阅 查看配置历史记录 (p. 59) 中的 `get-resource-config-history` Amazon CLI 命令生成的输出。

如果事件是针对定期评估而发布的，则值是一个包含 JSON 对象的字符串。该对象包含关于已触发的评估的信息。

对于每种类型的事件，函数必须通过 JSON 解析程序解析字符串，以便能够评估其内容，如下面的 Node.js 示例中所示：

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

函数会将其作为评估逻辑的一部分来处理的键/值对。使用时，您可以定义参数Amazon Config控制台以创建自定义 Lambda 规则。您也可以使用 `PutConfigRule` Amazon Config API 请求中的 `InputParameters` 属性或 `put-config-rule` Amazon CLI 命令来定义参数。

参数的 JSON 代码包含在字符串中，因此，函数必须通过 JSON 解析程序解析字符串，以便能够评估其内容，如下面的 Node.js 示例中所示：

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

函数必须通过 `PutEvaluations` 调用传递给 Amazon Config 的令牌。

`eventLeftScope`

表明要评估的 Amazon 资源是否已从规则范围内删除的布尔值。如果值为 `true`，则该函数表示可通过传递 `NOT_APPLICABLE` 作为 `ComplianceType` 调用中的 `PutEvaluations` 属性值来忽略评估。

`executionRoleArn`

分配给的 IAM 角色的 ARNAmazon Config.

`configRuleArn`

Amazon Config 分配给规则的 ARN。

`configRuleName`

您向导致 Amazon Config 发布事件并调用函数的规则分配的名称。

`configRuleId`

Amazon Config 分配给规则的 ID。

`accountId`

拥有规则的 Amazon 账户的 ID。

`version`

Amazon 分配的版本号。如果 Amazon 向 Amazon Config 事件添加属性，则版本号会递增。如果函数需要仅在匹配或超过特定版本的事件中的属性，则该函数可以检查此属性的值。

Amazon Config 事件的当前版本为 1.0。

管理您的 Amazon Config 规则

您可以使用 Amazon Config 控制台、Amazon CLI 和 Amazon Config API 来查看、添加和删除您的规则。

目录

添加、查看、更新和删除规则（控制台）

在 Rules 页面上，您可以查看您账户中的区域规则。您还可以查看每个规则的评估状态。

查看您的规则

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在 Amazon Web Services Management Console中，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关受支持的地区的列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
3. 选择 Rules。这些区域有：Rule页面显示了当前存在的所有规则Amazon Web Services 账户. 它列出了每个规则的名称、关联的补救措施和合规性状态。
   - 选择 Add rule 以开始创建规则。
   - 选择规则以查看其设置，或者选择规则并查看详细信息.
   - 当规则评估资源时，请查看规则的合规性状态。
   - 选择规则然后编辑规则以更改规则的配置设置并为不合规规则设置修正操作。

更新规则

1. 选择规则然后编辑规则对于您要更新的规则。
2. 修改上的设置编辑规则页面来根据需要更改您的规则。
3. 选择 Save（保存）。

删除一项规则

1. 从表中选择您要删除的规则。
2. 从操作下拉列表，选择删除规则.
3. 出现提示时，键入 “Delete”（区分大小写）然后选择Delete.

添加一项规则

如果您选择 Add rule，可以在 AmazonAdd rule 页面上查看可用的 托管规则。您还可以创建自己的自定义规则。

1. 如果您要创建自己的规则，请选择 Add custom rule，然后按照自定义 Lambda 规则（一般示例） (p. 188)中的过程操作。
2. 要添加托管规则，请在该页面上选择一个规则，然后按照使用 Amazon Config 托管规则 (p. 181)中的过程操作。

在 Add rule 页面上，可以执行以下操作：

- 选择 Add custom rule 以创建自己的规则。

- 在搜索字段中键入，以便按规则名称、描述或标签筛选结果。例如，键入 EC2 可返回评估 EC2 资源类型的规则，或者键入 periodic 可返回具有定期触发器的规则。键入“new”可搜索新添加的规则。有关触发器类型的更多信息，请参阅为 Amazon Config 规则指定触发器 (p. 122)。
- 通过选择箭头按字母顺序重新排序结果名称标签。
- 选择箭头图标可查看下一页规则。
- 查看最近添加的标记为的规则New.
- 有关标签来确定规则所评估的资源类型以及规则是否具有定期触发器。

查看、更新和删除规则 (Amazon CLI)

查看您的规则

- 使用 `describe-config-rules` 命令：

```
$ aws configservice describe-config-rules
```

Amazon Config 将返回您的所有规则的详细信息。

更新规则

1. 使用包含 `--generate-cli-skeleton` 参数的 `put-config-rule` 命令来创建包含您的规则参数的本地 JSON 文件：

```
$ aws configservice put-config-rule --generate-cli-skeleton > putConfigRule.json
```

2. 在文本编辑器中打开该 JSON 文件，然后删除不需要更新的所有参数，不过以下内容例外：
   - 至少包括以下参数之一以确定规则：

     `ConfigRuleName`, `ConfigRuleArn`, 或者 `ConfigRuleId`.
   - 如果您要更新自定义规则，则必须包含 `Source` 对象及其参数。
3. 填写剩余参数的值。要引用规则的详细信息，请使用 describe-config-rules 命令。

   例如，以下 JSON 代码可以更新自定义规则范围内的资源类型：

```
{
  "ConfigRule": {
    "ConfigRuleName": "ConfigRuleName",
    "Scope": {
      "ComplianceResourceTypes": [
        "AWS::EC2::Instance",
        "AWS::EC2::Volume",
        "AWS::EC2::VPC"
      ]
    },
    "Source": {
      "Owner": "CUSTOM_LAMBDA",
      "SourceIdentifier": "arn:aws:lambda:us-
east-2:123456789012:function:ConfigRuleName",
      "SourceDetails": [
        {
          "EventSource": "aws.config",
          "MessageType": "ConfigurationItemChangeNotification"
        }
      ]
    }
```

```
  }
}
```

4. 使用包含 `--cli-input-json` 参数的 `put-config-rule` 命令将您的 JSON 配置传递到 Amazon Config：

```
$ aws configservice put-config-rule --cli-input-json file://putConfigRule.json
```

5. 要验证您是否成功更新了规则，请使用 describe-config-rules 命令查看该规则的配置：

```
$ aws configservice describe-config-rules --config-rule-name ConfigRuleName
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "ConfigRuleName": "ConfigRuleName",
            "ConfigRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-nnnnnn",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-2:123456789012:function:ConfigRuleName",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC"
                ]
            },
            "ConfigRuleId": "config-rule-nnnnnn"
        }
    ]
}
```

删除一项规则

- 使用以下示例中所示的 `delete-config-rule` 命令：

```
$ aws configservice delete-config-rule --config-rule-name ConfigRuleName
```

查看、更新和删除规则 (API)

查看您的规则

使用DescribeConfigRuleaction.

更新或添加规则

使用PutConfigRuleaction.

删除规则

使用DeleteConfigRuleaction.

Note

如果一个规则创建无效的评估结果，您可能希望在修复该规则并运行新评估之前删除这些结果。有关更多信息，请参阅删除评估结果 (p. 209)。

评估您的资源

当您创建自定义规则或使用托管规则时，Amazon Config 按照这些规则评估您的资源。您可以按照您的规则对资源进行按需评估。例如，当您创建自定义规则并且希望验证 Amazon Config 是否正确评估您的资源或确定 Amazon Lambda 函数的评估逻辑是否有问题时，这会很有用。

示例

1. 您创建一个自定义规则，用以评估您的 IAM 用户是否具有有效的访问密钥。
2. Amazon Config 按照您的自定义规则评估资源。
3. 在您的账户中存在一个没有有效访问密钥的 IAM 用户。您的规则不正确将此资源标记为不合规。
4. 您修复规则并重新开始评估。
5. 由于您修复了规则，规则正确评估您的资源，并将 IAM 用户资源标记为不合规。

评估您的资源（控制台）

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在 Amazon Web Services Management Console菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关受支持的地区的列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
3. 在导航窗格中，选择 Rules (规则)。这些区域有：Rule页面显示每个规则的名称、关联的修正措施和合规性状态。
4. 从表中选择规则。
5. 从操作下拉列表中，选择重新评估.
6. Amazon Config 开始按照您的规则评估资源。

Note

您可以按照每分钟一个规则的频率重新计算。您必须等待 Amazon Config 完成您的规则的评估，然后您才能开始另一个评估。如果规则同时被更新或同时被删除，您将无法运行评估。

评估您的资源 (CLI)

- 使用 start-config-rules-evaluation 命令。

```
$ aws configservice start-config-rules-evaluation --config-rule-names ConfigRuleName
```

Amazon Config 开始按照您的规则评估记录的资源配置。

您还可以在请求中指定多个规则。

```
aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

评估您的资源 (API)

使用 StartConfigRulesEvaluation 操作。

删除评估结果

在 Amazon Config 评估您的规则后，您可以在该规则的 Rules (规则) 页或 Rules details (规则详细信息) 页上查看评估结果。如果评估结果不正确，或者您要重新评估，您可以删除该规则的当前评估结果。例如，如果您的规则错误地评估您的资源或从您最近已从账户中删除资源，您可以删除评估结果，然后运行新的评估。

删除评估结果（控制台）

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 在 Amazon Web Services Management Console菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关受支持的地区的列表，请参阅Amazon Config区域和终端节点中的Amazon Web Services 一般参考.
3. 在导航窗格中，选择 Rules (规则)。这些区域有：Rule页面显示每个规则的名称、关联的修正措施和合规性状态。
4. 从表中选择规则。
5. 从操作下拉列表，选择删除结果.
6. 出现提示时，键入 “Delete”（区分大小写）然后选择Delete. 删除的评估是无法检索的。
7. 在评估结果被删除后，您可以手动开始新的评估。

删除评估结果 (CLI)

- 使用 delete-evaluation-results 命令：

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

  Amazon Config 删除规则的评估结果。

删除评估结果 (API)

使用DeleteEvaluation结果action.

跨组织内的所有账户启用 Amazon Config 规则

Amazon Config 使您可以跨组织内的所有 Amazon 账户管理 Amazon Config 规则。您可以：

- 跨组织内的所有账户集中创建、更新和删除 Amazon Config 规则。

- 跨所有账户部署常用的一组 Amazon Config 规则，并指定不应创建 Amazon Config 规则的账户。
- 从 Amazon Organizations 的主账户中使用 API 确保组织的成员账户无法修改底层 Amazon Config 规则，从而强制实施监管。

> **Note**
>
> 适用于跨不同区域的部署
> 用于跨账户部署规则和一致性包的 API 调用是特定于区域的。在组织层面，如果您想在其他区域部署规则，则需要将 API 调用的上下文更改为其他区域。例如，要在美国东部（弗吉尼亚北部）部署规则，请将区域更改为美国东部（弗吉尼亚北部），然后调用`PutOrganizationConfigRule`.
> 对于组织内的账户
> 如果有新账户加入组织，则规则或一致性包将部署到该账户。当账户离开组织时，规则或一致性包将被删除。
> 如果您在组织管理员帐户中部署组织规则或一致性包，然后建立委派管理员并在委派管理员帐户中部署组织规则或一致性包，您将无法在来自委派管理员帐户的组织管理员帐户，或者在组织管理员帐户的委派管理员帐户中查看组织规则或一致性包。这些区域有：DescribeOrganizationConfigRules和DescribeOrganizationConformancePacksAPI 只能查看从调用这些 API 的账户内部部署的组织相关资源并与之交互。
> 为组织提供新账户的重试机制
> 如果记录器不可用，则只有在将帐户添加到组织后 7 小时内才会重试现有组织规则和一致性包的部署。如果在向组织添加帐户后的 7 小时内没有记录器，则需要创建一个记录器。

确保在使用以下 API 跨组织内的所有 Amazon 账户管理 Amazon Config 规则之前，Amazon Config 记录已打开：

- PutOrganizationConfigRule，为整个组织评估添加或更新组织 Config 规则，以评估您的Amazon资源符合您所需的配置。
- DescribeOrganizationConfigRules，返回组织配置规则的列表。
- GetOrganizationConfigRuleDetailedStatus返回给定组织配置规则的组织内每个成员账户的详细状态。
- GetOrganizationCustomRulePolicy，返回包含组织配置自定义策略规则逻辑的策略定义。
- DescribeOrganizationConfigRuleStatuses，为组织提供组织配置规则部署状态。
- DeleteOrganizationConfigRule，从该组织的所有成员账户中删除指定的组织 Config 规则及其所有评估结果。

区域支持

部署Amazon Config跨成员账户的规则Amazon以下区域支持组织。

区域名称	区域	Endpoint	协议
Asia Pacific (Seoul)	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacific (Tokyo)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS

区域名称	区域	Endpoint	协议
Canada (Central)	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
Europe (Ireland)	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
South America (São Paulo)	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
US East (Ohio)	us-east-2	config.us-east-2.amazonaws.com	HTTPS
US West (N. California)	us-west-1	config.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	config.us-west-2.amazonaws.com	HTTPS

修正不合规Amazon资源Amazon Config Rules

Amazon Config 允许您修正被 Amazon Config Rules 评估为不合规的资源。Amazon Config 使用 Amazon Systems Manager 自动化文档应用修正。这些文档定义了对不合规执行的操作Amazon评估的资源Amazon Config Rules. 您可以使用 Amazon Web Services Management Console或 API 来关联 SSM 文档。

Amazon Config 提供了一组具有修正操作的托管自动化文档。您也可以创建自定义自动化文档并将其与 Amazon Config 规则关联。

要将修正应用于不合规的资源，您可以从预先填充的列表中选择要关联的修正操作，也可以使用 SSM 文档创建自己的自定义修正操作。Amazon Config 在 Amazon Web Services Management Console 中提供了建议的修正操作清单。

在Amazon Web Services Management Console，你可以选择手动要么自动通过将补救措施与关联来修复不合规的资源Amazon Config规则。借助所有修正操作，您可以选择手动或自动修正。

主题

- 管理修正 (API) (p. 213)

先决条件

在开始对不合规资源应用修正之前，您必须选择一条规则并针对该规则设置修正（手动或自动）。

设置手动修正（控制台）

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 选择Rule在左边然后在Rule页面上，选择添加规则向规则列表中添加新规则

   对于现有规则，从规则列表中选择不合规规则，然后选择操作下拉列表。
3. 从操作下拉列表中，选择管理修正. 选择 “手动修正”，然后从推荐列表中选择适当的修正操作。

   Note

   你只能管理非服务链接的补救Amazon Config规则。有关更多信息，请参阅 。服务相关AmazonRule.

   根据所选的修正操作，您将会看到特定参数，或者看不到任何参数。
4. （可选）：如果要将不合规资源的资源 ID 传递给修正操作，请选择 Resource ID parameter (资源 ID 参数)。如果选中，则在运行时会将该参数替换为要修正的资源的 ID。

   每个参数都具有静态值或动态值。如果未从下拉列表中选择特定资源 ID 参数，则可以为每个键输入值。如果从下拉列表中选择资源 ID 参数，则可以为除所选资源 ID 参数之外的所有其他键输入值。
5. 选择 Save（保存）。此时将显示 Rules (规则) 页面。

   Note

   要对失败的修复操作进行故障排除，可以运行Amazon命令行界面命令`describe-remediation-execution-status`获取资源集修复执行的详细视图。详细信息包括修正执行步骤的状态、时间戳，以及失败步骤的任何错误消息。

设置自动修正（控制台）

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 选择左侧的 Rules (规则)，然后在 Rules (规则) 页面上选择 Add Rule (添加规则)，然后向规则列表中添加新规则。

   对于现有规则，从规则列表中选择不合规规则，然后选择操作下拉列表。
3. 从操作下拉列表中，选择管理修正. 选择 “自动修正”，然后从推荐列表中选择适当的修正操作。

   Note

   你只能管理非服务链接的补救Amazon Config规则。有关更多信息，请参阅 。服务相关AmazonRule.

   根据所选的修正操作，您将会看到特定参数，或者看不到任何参数。
4. 选择 Auto remediation (自动修正) 以自动修正不合规的资源。

   如果在自动修正后资源仍然不合规，则可以设置规则以再次尝试自动修正。输入所需的重试次数和秒数。

Note

多次运行修正脚本会有关联的成本。

5. （可选）：如果要将不合规资源的资源 ID 传递给修正操作，请选择 Resource ID parameter (资源 ID 参数)。如果选中，则在运行时会将该参数替换为要修正的资源的 ID。

   每个参数都具有静态值或动态值。如果未从下拉列表中选择特定资源 ID 参数，则可以为每个键输入值。如果从下拉列表中选择资源 ID 参数，则可以为除所选资源 ID 参数之外的所有其他键输入值。
6. 选择 Save（保存）。此时将显示 Rules (规则) 页面。

Note

要对失败的修复操作进行故障排除，可以运行Amazon命令行界面命令`describe-remediation-execution-status`获取资源集修复执行的详细视图。详细信息包括修正执行步骤的状态、时间戳，以及失败步骤的任何错误消息。

删除修正操作（控制台）

要删除规则，必须首先删除与该规则关联的修正操作。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/。
2. 选择Rule在左边然后在Rule页面上，从规则列表中选择规则，然后选择查看详细信息.
3. 在存储库的*#####*页面上，转至修复操作部分。展开部分以查看更多详细信息。
4. 在修复操作部分中，选择Delete然后确认删除操作。

   Note

   如果修正正在进行中，修复操作不会被删除。一旦选择删除修正操作，您将无法检索修正操作。删除修正操作不会删除相关规则。

   如果删除了修复操作，资源 ID 参数将为空并显示 N/A。在Rule页面中，将显示修复操作列未设置对于关联的规则。

管理修正 (API)

手动修正

使用以下 Amazon Config API 操作来管理修正：

- DeleteRemediationConfiguration
- DescribeRemediationConfigurations
- DescribeRemediationExecutionStatus
- PutRemediationConfigurations
- StartRemediationExecution

自动修正

使用以下 Amazon Config API 操作来管理自动修正：

- PutRemediationExceptions

- DescribeRemediationExceptions
- DeleteRemediationExceptions

Amazon Config 中的安全性

Amazon 十分重视云安全性。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 Amazon 客户，您也将从这些数据中心和网络架构受益。

安全性是 Amazon 和您的共同责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全性 – Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础设施。Amazon 还向您提供可安全使用的服务。作为Amazon 合规性计划的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于的合规性计划Amazon Config, 请参阅Amazon合规性计划范围内的服务.
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其它因素负责，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。

此文档将帮助您了解如何在使用 Amazon Config 时应用责任共担模型 以下主题说明如何配置 Amazon Config 以实现您的安全性和合规性目标。

主题

Amazon Config 中的数据保护

这些区域有：Amazon 责任共担模式适用于中的数据保护AmazonConfig. 如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 Amazon Web Services 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。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户 凭证并使用 Amazon Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 Amazon 资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 Amazon CloudTrail 设置 API 和用户活动日志记录。
- 使用 Amazon 加密解决方案以及 Amazon 服务中的所有默认安全控制。
- 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 Simple Storage Service（Amazon S3）中的个人数据。

- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 终端节点。有关可用的 FIPS 终端节点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括使用时AmazonConfig 或其他Amazon服务使用控制台、API、Amazon CLI，或者Amazon开发工具包。您在用于名称的标签或自由格式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，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

静态数据加密

使用透明的服务器端加密，静态加密数据。这样可以帮助减少在保护敏感数据时涉及的操作负担和复杂性。通过静态加密，您可以构建符合加密合规性和法规要求的安全敏感型应用程序。

传输中的数据的加密

收集和访问的数据Amazon Config只只只只只只只只只只只只只只只只只只只只只只只只只只只只

Amazon Identity and Access Management

Amazon Config已与 集成Amazon Identity and Access Management(IAM)，它允许您创建权限策略，以附加到您的 IAM 角色、Amazon S3 存储桶和 Amazon Simple Notification Service (Amazon SNS) 主题。您可以使用Amazon Identity and Access Management来创建Amazon Config要附加到 IAM 角色的权限策略。策略是用于授予 Amazon Config 权限的一组语句。

> Important
>
> 我们认为最佳做法是，不要将根账户凭证用于在 Amazon 中执行日常工作。相反，我们建议您创建具有适当权限的 IAM 管理员组，为您组织中需要执行管理任务的人员 (包括您自己) 创建 IAM 用户，并将这些用户添加到管理员组。有关更多信息，请参阅 。IAM 最佳实践中的IAM 用户指南指南。

前两个主题控制用户对 Amazon Config 的权限，后面的主题提供有关 Amazon Config 所需的权限的准确配置信息。这些主题提供了建议与Amazon Config控制台和Amazon Command Line Interface.

主题

授予 Amazon Config 管理权限

允许用户管理Amazon Config，您必须向 IAM 用户授予显式权限以使其能够执行与Amazon Config任务。在大多数情况下，您可以使用包含预定义权限的 Amazon 托管策略来执行此操作。

Note

您授予用户执行的权限Amazon Config管理任务与以下权限不同Amazon Config本身需要，以便将日志文件传输到 Amazon S3 存储桶或将通知发送到 Amazon SNS 主题。

设置和管理 Amazon Config 的用户必须具有完全访问权限。通过完全访问权限，用户可以提供 Amazon S3 和 Amazon SNS 终端节点Amazon Config向传送数据，为创建角色Amazon Config，然后打开和关闭录制。

使用 Amazon Config 但无需设置 Amazon Config 的用户应获得只读权限。如果具有只读权限，用户可以查找资源的配置或者按标签搜索资源。

一种典型方法是创建具有适当权限的 IAM 组，然后将单个 IAM 用户添加到该组。例如，您可以为应具备完全访问权限的用户创建 IAM 组Amazon Config操作，并为应能够查看配置而不是创建或更改角色的用户创建单独的组。

目录

为创建 IAM 组和用户Amazon Config访问

1. 登录到Amazon Identity and Access Management(IAM) 控制台位于https://console.aws.amazon.com/iam.
2. 在控制面板的导航窗格中，选择 Groups，然后选择 Create New Group。
3. 键入名称，然后选择 Next Step。
4. 在存储库的附加策略页面上，找到并选择AWSConfigUserAccess. 此策略为用户提供使用 Amazon Config 的访问权限，包括按资源上的标签进行搜索，以及读取所有标签。这不提供配置 Amazon Config 的权限（这需要管理权限）。

   Note

   您还可创建用于授予单个操作的权限的自定义策略。有关更多信息，请参阅 向 Amazon Config 用户授予自定义权限 (p. 227)。
5. 选择 Next Step。
6. 查看您即将创建的组的信息。

   Note

   您可以编辑组名，但需要再次选择策略。
7. 选择 Create Group（创建组）。已创建的组将显示在组列表中。
8. 选择您创建的组名，选择 Group Actions，然后选择 Add Users to Group。
9. 在存储库的将用户添加到组页面上，选择现有的 IAM 用户，然后选择添加用户. 如果您还没有 IAM 用户，请选择创建新用户，输入用户名，然后选择Create.
10. 如果创建了新用户，请在导航窗格中选择 Users，然后针对每个用户完成以下操作：
    a. 选择用户。
    b. 如果用户将使用控制台管理 Amazon Config，则在 Security Credentials 选项卡中选择 Manage Password，然后为用户创建密码。
    c. 如果用户将使用 Amazon CLI 或 API 管理 Amazon Config，并且如果您尚未创建访问密钥，则在 Security Credentials (安全凭证) 选项卡中选择 Manage Access Keys (管理访问密钥)，然后创建访问密钥。将密钥存储在安全位置。

d. 为每个用户提供证书（访问密钥或密码）。

授予完全访问权限以进行 Amazon Config 访问

1. 登录到Amazon Identity and Access Management(IAM) 控制台位于https://console.aws.amazon.com/iam.
2. 在导航窗格中选择 Policies，然后选择 Create Policy。这将打开 Plication (策略编辑器)。
3. 您可以使用可视化编辑器选项卡或 JSON 选项卡创建您自己的自定义策略。您可以选择...导入托管策略使用您自己创建的策略或由管理的策略的权限Amazon.
4. Select下一步:标签.
5. 添加您希望策略具有的任何标签。
6. SelectNext: 审核.
7. 键入策略名称和描述（可选）。查看策略提供的权限。
8. 选择 Create Policy (创建策略)。
9. 在策略列表中，选择您创建的策略。您可以使用 Filter 菜单和 Search 框来查找策略。
10. 选择您创建的策略旁边的单选按钮，然后选择操作在右上角。在此下拉列表中选择Attach.
11. 选择用户、组或角色，然后选择 Attach Policy。您可以使用 Filter 菜单和 Search 框来筛选列表。
12. Select附加策略.

Note

您也可以从 IAM 控制台创建一个内联策略并将该策略附加到 IAM 用户、组或角色，而不创建托管策略。有关更多信息，请参阅 。使用内联策略中的IAM 用户指南.

其他资源

要了解有关创建 IAM 用户、组、策略和权限的更多信息，请参阅 IAM 用户指南中的使用控制台创建管理员组和权限与策略。

分配给的 IAM 角色权限Amazon Config

网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的Amazon Identity and Access Management(IAM) 角色允许您定义一组权限。Amazon Config代入您分配给它的角色，将写入您的 S3 存储桶、发布到您的 SNS 主题，以及创建`Describe`要么`List`API 请求获取您的配置详细信息Amazon资源的费用。有关 IAM 角色的更多信息，请参阅IAM 角色中的IAM 用户指南.

当您使用以下应用程序时：Amazon Config控制台，用于创建或更新 IAM 角色，Amazon Config会自动为您附加所需权限。有关更多信息，请参阅 使用控制台设置 Amazon Config (p. 27)。

目录

创建 IAM 角色策略

当您使用以下应用程序时：Amazon Config控制台创建 IAM 角色，Amazon Config会自动为您附加该角色所需的权限。

在使用Amazon CLI设置Amazon Config或者您要更新一个现有 IAM 角色，您必须手动更新策略以允许Amazon Config要访问您的 S3 存储桶，请发布到您的 SNS 主题，并获取有关您资源的配置详细信息。

将一个 IAM 信任策略添加到您的角色

您可以创建一个 IAM 信任策略来启用Amazon Config以代入一个角色并利用该角色跟踪您的资源。有关信任策略的更多信息，请参阅代入一个角色中的IAM 用户指南.

下面是 Amazon Config 角色的示例信任策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

您可以使用AWS:SourceAccount上述 IAM 角色信任关系中的条件，以限制 Config 服务委托人仅与Amazon代表特定账户执行操作时的 IAM 角色。

Amazon Config也支持AWS:SourceArn条件，该条件限制 Config 服务委托人仅在代表拥有账户执行操作时担任 IAM 角色。使用Amazon Config服务委托人，AWS:SourceArn属性将始终设置为arn:aws:config:sourceRegion:sourceAccountID:*哪里sourceRegion是配置记录器的区域，sourceAccountID是包含配置记录器的帐户的 ID。有关Amazon Config配置记录器请参阅管理配置记录器. 例如，添加以下条件限制 Config 服务委托人仅代表配置记录器在us-east-1账户中的区域123456789012："ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}.

Amazon S3 存储桶的 IAM 角色策略

以下示例策略授予的示例Amazon Config访问您的 Amazon S3 存储桶的权限：

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*"
```

```
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::myBucketName"
    }
  ]
}
```

KMS 密钥的 IAM 角色策略

以下示例策略授予的示例Amazon Config对 S3 存储桶交付的新对象使用基于 KMS 的加密的权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

适用于Amazon SNS 的 IAM 角色策略主题

以下示例策略授予 Amazon Config 权限以访问您的 SNS 主题：

```
{
  "Version": "2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"mySNStopicARN"
     }
    ]
}
```

如果您的 SNS 主题已加密，请参阅配置Amazon KMSPermissions (权限)中的Amazon Simple Notifice.

用于获取配置详细信息的 IAM 角色策略

录制你的Amazon资源配置，Amazon Config需要 IAM 权限才能获取有关您的资源的配置详细信息。

使用Amazon管理的策略AWS_ConfigRole并将其附加到您分配给的 IAM 角色Amazon Config.Amazon每次都更新此策略Amazon Config添加了对以下应用程序的支持：Amazon资源类型，这意味着Amazon Config只要角色附加了此托管策略，就将继续拥有必需权限来获取配置详细信息。

如果您使用控制台创建或更新角色，Amazon Config将附加到AWS_ConfigRole为您。

如果您将Amazon CLI，请使用`attach-role-policy`命令并指定的 Amazon 资源名称 (ARN)AWS_ConfigRole：

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn arn:aws:iam::aws:policy/
service-role/AWS_ConfigRole
```

管理 S3 存储桶录制权限

Amazon Config当创建、更新或删除 S3 存储桶时进行记录并发送通知。

建议您使用`AWSServiceRoleForConfig`（请参阅对 使用服务相关角色Amazon Config) 或使用`AWS_ConfigRole`管理的策略。有关配置录制的最佳做法的更多信息，请参阅Amazon Config最佳实践.

如果您需要管理存储桶记录的对象级权限，请确保在 S3 存储桶策略中提供`config.amazonaws.com`（的 Amazon Config服务主体名称）访问所有 S3 相关权限`AWS_ConfigRole`管理的策略。有关更多信息，请参阅 。Amazon S3 存储桶的权限.

Amazon S3 存储桶的权限

默认情况下，所有 Amazon S3 存储桶和对象都是私有的。只有资源所有者是Amazon创建存储桶的账户可以访问该存储桶。但是，资源所有者可以选择将访问权限授予其他资源和用户。要授予访问权限，其中一种方法是编写访问策略。

如果Amazon Config自动为您创建 Amazon S3 存储桶（例如，如果您使用Amazon Config控制台设置您的传输通道），这些权限会自动添加到 Amazon S3 存储桶。但是，如果您指定现有的 Amazon S3 存储桶，则您必须确保该 S3 存储桶具有相应权限。

> Note
>
> 对象不继承其存储桶的权限。例如，如果您创建了一个存储桶并授予一个用户写入权限，则将无法访问此用户的对象，除非此用户显式授予您访问权限。

目录

使用 IAM 角色时 Amazon S3 存储桶的必需权限

何时Amazon Config将配置信息 (历史记录文件和快照) 发送到您账户的 Amazon S3 存储桶，它会代入您在设置时分配的 IAM 角色Amazon Config. 何时Amazon Config将配置信息发送到另一账户的 Amazon S3 存储桶，它会首先尝试使用 IAM 角色，但如果该存储桶的访问策略未授予此存储桶的访问策略未授予此次尝试将会失败`WRITE`对 IAM 角色的访问权限。在这种情况下，Amazon Config 会再次发送这些信息，这次会以 Amazon Config 服务委托人的身份发送。该访问策略必须先向名称为 `config.amazonaws.com` 的委托人授予 `WRITE` 访问权限，然后才能成功传递。这样一来，Amazon Config 便会成为其向 S3 存储桶传递的对象的所有者。您必须将下面第 6 步中提到的一个访问策略附加到另一账户的 Amazon S3 存储桶，以向授予权限Amazon Config对 Amazon S3 存储桶的访问权限。

优化前Amazon Config可将日志传送至 Amazon S3 存储桶Amazon Config检查存储桶是否存在以及存储桶在哪个Amazon存储桶所在的区域。Amazon Config尝试调用 Amazon S3HeadBucket用于检查存储桶是否存在以及获取存储桶区域的 API。如果在执行位置检查时未提供定位存储桶所需的权限，您将在 Amazon CloudTrail 日志中看到 `AccessDenied` 错误。但是，如果您未提供存储桶定位权限，日志会成功传输到 Amazon S3 存储桶。

使用服务相关角色时的 Amazon S3 存储桶的必需权限

这些区域有：Amazon Config服务相关角色无权将对象放入到 Amazon S3 存储桶。所以，如果你设置 Amazon Config使用服务相关角色，Amazon Config将发送配置项作为Amazon Config服务委托人：您需要将下面第 6 步中提到的一个访问策略附加到您自己的账户或其他账户的 Amazon S3 存储桶，以进行授予授予权限Amazon Config对 Amazon S3 存储桶的访问权限。

授权Amazon Config对 Amazon S3 存储桶的访问权限

按照以下步骤向您自己的账户或其他账户的 Amazon S3 存储桶添加访问策略。访问策略允许Amazon Config以将配置信息发送到 Amazon S3 存储桶。

1. 使用该 S3 存储桶所属的账户登录 Amazon Web Services Management Console。
2. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
3. 选择您希望 Amazon Config 用来传递配置项的存储桶，然后选择 Properties (属性)。
4. 请选择权限。
5. 选择 Edit Bucket Policy。
6. 将以下策略复制到 Bucket Policy Editor 窗口中：

   Important

   允许时作为最佳安全实践Amazon Config访问 Amazon S3 存储桶，我们强烈建议您在存储桶策略中使用`AWS:SourceAccount`条件。如果您的现有存储桶策略未遵循此安全最佳实践，我们强烈建议您编辑该存储桶策略以包含此保护。这样可以确保Amazon Config仅被授予代表预期用户的访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
```

```
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

Note

Amazon Config拥有的Amazon并且不专门属于你的一个Amazon您的账户或关联账户Amazon组织。这意味着Amazon Config正在发送配置项作为Amazon Config服务委托人（例如您在设置时分配的 IAM 角色时Amazon Config没有`WRITE`访问存储桶或在您设置时访问Amazon Config若要使用服务相关角色），则该服务将不适用于基于组织 ID 或组织单位的条件。

Note

向您的 IAM 角色授予权限而不是授予权限时Amazon Config服务主体名称 (SPN)，请确保您的 IAM 角色具有`PutObjectACL`跨账户存储桶的权限，以避免权限不足错误。请参阅 IAM 角色策略示例： Amazon S3 存储桶的 IAM 角色策略 (p. 219).

7. 替换存储桶策略中的以下值：
   - *`targetBucketName`*— 存放的 Amazon S3 存储桶的名称Amazon Config将交付配置项目。
   - *`[##] ##`*— Amazon S3 对象键的可选附加内容，可帮助在存储桶中创建类似于文件夹的组织结构。
   - *`## AccountID`*— 该账户的账户 IDAmazon Config将配置项传送到目标存储桶。
8. 选择 Save，然后选择 Close。

您可以使用`AWS:SourceAccount`条件，以限制 Config 服务委托人仅在代表特定账户执行操作时与 Amazon S3 存储桶进行交互。如果你打算设置Amazon Config在来自同一组织的多个账户中将配置项目传输到单个 Amazon S3 存储桶时，我们建议使用 IAM 角色而不是服务相关角色，以便您可以使用Amazon Organizations条件键例如`AWS:PrincipalOrgID`. 有关管理要与一起使用的 IAM 角色的访问权限的更多信息Amazon Config, 请参阅分配给的 IAM 角色权限Amazon Config. 有关管理的访问权限的更多信息Amazon Organizations, 请参阅管理您的访问权限Amazon组织.

Amazon Config也支持`AWS:SourceArn`条件，该条件限制 Config 服务委托人仅在代表特定用户执行操作时与 Amazon S3 存储桶交互Amazon Config交付渠道。使用Amazon Config服务委托人，`AWS:SourceArn`属性将始终设置为`arn:aws:config:sourceRegion:sourceAccountID:*`哪里`sourceRegion`是传递通道的区域`sourceAccountID`是包含传送渠道的账户的 ID。有关Amazon Config配送渠道，请参阅管理传递通道. 例如，添加以下条件以限制 Config 服务委托人仅代表传输通道与您的 Amazon S3 存储桶进行交互`us-east-1`账户中的区域`123456789012`：`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`.

KMS 密钥的权限

为 Amazon S3 KMS 密钥创建策略，该策略允许您对传输的对象使用基于 KMS 的加密Amazon Config用于 S3 存储桶交付。

目录

使用 IAM 角色时 KMS 密钥所需的权限（S3 存储桶交付）

如果您设置Amazon Config利用 IAM 角色，您可以将以下权限策略附加到 KMS 密钥：

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

Note

如果是 IAM 角色、Amazon S3 存储桶策略或Amazon KMS密钥不提供适当的访问权限Amazon Config，那么Amazon Config尝试将配置信息发送到 Amazon S3 存储桶将失败。在这种情况下，Amazon Config 会再次发送这些信息，这次会以 Amazon Config 服务委托人的身份发送。对于这种情况，您必须将如下所述的权限策略附加到Amazon KMS要授予的密钥Amazon Config在将信息传输到 Amazon S3 存储桶时使用密钥的权限。

使用服务相关角色（S3 存储桶交付）时的 KMS 密钥的必需权限

如果您设置Amazon Config使用服务相关角色，您需要将以下权限策略附加到 KMS 密钥。

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
```

```
                }
            }
        }
    ]
}
```

替换密钥策略中的以下值：

- *mykmsKeyarn*— 的 ARNAmazon KMS用于对 Amazon S3 存储桶中的数据进行加密的密钥Amazon Config将向传送配置项目。
- *## AccountID*— 该账户的账户 IDAmazon Config将向传送配置项目。

您可以使用AWS:SourceAccount条件Amazon KMS上面的密钥策略限制 Config 服务主体只能与Amazon KMS代表特定的账户执行操作时的密钥。

Amazon Config也支持AWS:SourceArn条件，该条件限制 Config 服务委托人仅在代表特定用户执行操作时与 Amazon S3 存储桶交互Amazon Config交付渠道。使用Amazon Config服务委托人，AWS:SourceArn属性将始终设置为arn:aws:config:sourceRegion:sourceAccountID:*哪里sourceRegion是传递通道的区域sourceAccountID是包含传送渠道的账户的 ID。有关Amazon Config配送渠道，请参阅管理传递通道. 例如，添加以下条件以限制 Config 服务委托人仅代表传输通道与您的 Amazon S3 存储桶进行交互us-east-1账户中的区域123456789012："ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}.

Amazon SNS 主题的权限

如果要配置，请使用本主题中的信息Amazon Config：传输不同账户拥有的 Amazon SNS 主题。Amazon Config必须具有将通知发送到 Amazon SNS 主题的必需权限。对于相同账户的设置，当Amazon Config控制台会创建 Amazon SNS 主题，或者您从自己的账户中选择一个 Amazon SNS 主题，Amazon Config确保 Amazon SNS 主题包含所需的权限并遵循安全最佳实践。

> **Note**
>
> Amazon Config目前仅支持相同区域和跨账户访问。用于补救的 SNS 主题Amazon Systems Manager(SSM) 文档或录制器传送通道的文档不能跨区域。

目录

使用 IAM 角色时 Amazon SNS 主题的必需权限

您可以将权限策略附加到不同账户拥有的 Amazon SNS 主题。如果您希望使用另一账户的 Amazon SNS 主题，请确保将以下策略附加到现有的 Amazon SNS 主题。

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
```

```
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

对于Resource键,*account-id*是Amazon主题所有者的账号。适用于*## id1*、*## id2*, 和*## id3*，请使用Amazon将数据发送到 Amazon SNS 主题的账户。你可以用适当的值替换*##*和*####*.

何时Amazon Config将通知发送到 Amazon SNS 主题，它会首先尝试使用 IAM 角色，但如果角色或Amazon账户没有发布到主题的许可。在本次活动中，Amazon Config会再次发送通知，这次会以 Config 服务委托人名称 (SPN) 的形式发送。在成功发布之前，主题的访问策略必须授予sns:Publish使用config.amazonaws.com委托人名称。您必须将下面提到的一个访问策略附加到 Amazon SNS 主题才能授予Amazon Config在 IAM 角色无权发布到该主题时访问 Amazon SNS 主题。

使用服务相关角色时Amazon SNS 主题的必需权限

授权Amazon Config访问Amazon SNS 主题，您将需要附加以下权限策略。这是因为 Config 服务主体名称 (SPN) 是必需的Amazon Config服务相关角色 (SLR)，用于从其他账户访问 Amazon SNS 主题。以下权限策略包含安全最佳实践，以确保Amazon Config仅通过限制对中列出的帐户的访问权限来代表预期用户访问资源AWS:SourceAccount条件。强烈建议使用此安全最佳实践。

对于同账户设置，当Amazon SNS 主题和 SLR 位于同一个账户，且Amazon SNS 策略授予 SLR"sns:Publish"权限，您无需使用Amazon ConfigSPN。以下权限策略和安全最佳实践适用于跨账户设置。

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

对于Resource键,*account-id*是Amazon主题所有者的账号。适用于*## id1*、*## id2*, 和*## id3*，请使用Amazon将数据发送到 Amazon SNS 主题的账户。你可以用适当的值替换*##*和*####*.

您可以使用AWS:SourceAccount条件，以限制Config 服务主体名称 (SPN) 在代表特定账户执行操作时仅与 Amazon SNS 主题进行交互。

Amazon Config也支持AWS:SourceArn条件，该条件限制 Config 服务主体名称 (SPN) 仅在代表特定用户执行操作时与 Amazon S3 存储桶交互Amazon Config交付渠道。使用 Config 服务主体名称 (SPN) 时，AWS:SourceArn属性将始终设置为arn:aws:config:sourceRegion:sourceAccountID:*哪里sourceRegion是传递通道的区域sourceAccountID是包含传送渠道的账户的 ID。有关Amazon Config配送渠道，请参阅管理传递通道. 例如，添加以下条件以限制 Config 服务委托人名称 (SPN) 仅代表传输通道与 Amazon S3 存储桶进行交互us-east-1账户中的区域123456789012："ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}.

Amazon SNS 主题问题排查

Amazon Config必须具有将通知发送到 Amazon SNS 主题的权限。如果 Amazon SNS 主题无法接收通知，请验证 IAM 角色是否具有Amazon Config假设一定有sns:Publish权限。

向 Amazon Config 用户授予自定义权限

Amazon Config 策略向使用 Amazon Config 的用户授予权限。如果您需要向用户授予不同权限，可将Amazon Config策略至 IAM 群组或用户。您可以编辑策略，使之包括或排除特定权限。您还可以创建自己的自定义策略。策略是一些 JSON 文档，它们定义了允许用户执行的操作以及允许用户对哪些资源执行这些操作。

目录

只读访问权限

以下示例演示了一个 Amazon 托管策略 AWSConfigUserAccess，该策略授予对 Amazon Config 的只读访问权。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

在这些策略语句中，Effect 元素指定是允许还是拒绝操作。Action 元素列出了允许用户执行的特定操作。Resource 元素列出允许用户对其执行这些操作的 Amazon 资源。对于控制对 Amazon Config 操作的访问的策略，Resource 元素始终设置为 * (一个表示“所有资源”的通配符) 。

`Action` 元素中的值对应于服务支持的 API。操作前附加了 `config:` 以表示其指的是 Amazon Config 操作。您可以在 `*` 元素中使用 `Action` 通配符，如以下示例所示：

- `"Action": ["config:*ConfigurationRecorder"]`

  这将允许所有Amazon Config以” 结尾的操作 ConfigurationRecorder“(`StartConfigurationRecorder`、`StopConfigurationRecorder`)。
- `"Action": ["config:*"]`

  这允许所有 Amazon Config 操作，但不允许其他 Amazon 服务的操作。
- `"Action": ["*"]`

  这将允许所有 Amazon 操作。此权限适合授予充当您账户的 Amazon 管理员的用户。

只读策略不对用户授予执行 `StartConfigurationRecorder`、`StopConfigurationRecorder` 和 `DeleteConfigurationRecorder` 操作的权限。不允许使用此策略的用户启动配置记录器、停止配置记录器或删除配置记录器。对于列表Amazon Config操作，请参阅Amazon ConfigAPI 参考.

完全访问权限

以下示例展示了一个授予对 Amazon Config 的完全访问权限的策略。它对用户授予执行所有 Amazon Config 操作的权限。它还允许用户管理 Amazon S3 存储桶中的文件，以及管理与用户关联的账户中的 Amazon SNS 主题。

> **Note**
>
> 此策略授予广泛的权限。在授予完全访问权限之前，请考虑最开始只授予最低权限，然后根据需要授予其他权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说是更好的做法。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
```

```
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
```

```
}
```

控制对多账户多区域数据聚合执行操作的用户权限

您可以使用资源级权限控制用户对多账户多区域数据聚合执行特定操作的能力。Amazon Config 多账户多区域数据聚合 API 支持资源级别权限。使用资源级别权限可以将访问/修改资源数据限制为特定用户。

例如，您希望将对资源数据的访问限制为特定用户。您可以创建两个聚合器`AccessibleAggregator`和`InAccessibleAggregator`. 然后，附加一个允许访问的 IAM 策略`AccessibleAggregator`.

在第一个策略中，您允许对您指定的配置 ARN 执行聚合器操作，例如 `DescribeConfigurationAggregators` 和 `DeleteConfigurationAggregator` 操作。在下面的示例中，配置 ARN 为 `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`。

```
{
        "Version": "2012-10-17",
        "Statement": [
        {
        "Sid": "ConfigReadOnly",
        "Effect": "Allow",
        "Action": [
            "config:PutConfigurationAggregator",
            "config:DescribePendingAggregationRequests",
            "config:DeletePendingAggregationRequest",
            "config:GetAggregateConfigRuleComplianceSummary",
            "config:DescribeAggregateComplianceByConfigRules",
            "config:GetAggregateComplianceDetailsByConfigRule",
            "config:DescribeConfigurationAggregators",
            "config:DescribeConfigurationAggregatorSourcesStatus",
            "config:DeleteConfigurationAggregator"
        ],
        "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs"
        }
    ]
}
```

在第二个策略中，您拒绝对您指定的配置 ARN 执行聚合器操作。在下面的示例中，配置 ARN 为 `arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-pokxzldx`。

```
{
        "Version": "2012-10-17",
        "Statement": [
        {
        "Sid": "ConfigReadOnly",
        "Effect": "Deny",
        "Action": [
            "config:PutConfigurationAggregator",
            "config:DescribePendingAggregationRequests",
            "config:DeletePendingAggregationRequest",
            "config:GetAggregateConfigRuleComplianceSummary",
            "config:DescribeAggregateComplianceByConfigRules",
            "config:GetAggregateComplianceDetailsByConfigRule",
            "config:DescribeConfigurationAggregators",
            "config:DescribeConfigurationAggregatorSourcesStatus",
```

```
            "config:DeleteConfigurationAggregator"
        ],
        "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-
aggregator-pokxzldx"
        }
    ]
}
```

如果开发人员组中的用户尝试针对您在第二个策略中指定的配置描述或删除配置聚合器，该用户会收到拒绝访问异常。

以下 Amazon CLI 示例说明用户如何创建两个聚合器，即 `AccessibleAggregator` 和 `InAccessibleAggregator`。

```
aws configservice describe-configuration-aggregators
```

该命令成功完成：

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-northeast-1:AccountID:config-
aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

Note

对于 account-aggregation-sources，输入要为其聚合数据的 Amazon 账户 ID 的逗号分隔的列表。用方括号将账户 ID 括起来，并确保对引号进行转义 (例如，"[{\"AccountIds\": [\"*AccountID1*\",\"*AccountID2*\",\"*AccountID3*\"],\"AllAwsRegions\": true}]")。

然后，用户创建 IAM 策略，以拒绝对的访问InAccessibleAggregator.

```
{
        "Version": "2012-10-17",
        "Statement": [
        {
        "Sid": "ConfigReadOnly",
        "Effect": "Deny",
        "Action": [
            "config:PutConfigurationAggregator",
            "config:DescribePendingAggregationRequests",
            "config:DeletePendingAggregationRequest",
            "config:GetAggregateConfigRuleComplianceSummary",
            "config:DescribeAggregateComplianceByConfigRules",
            "config:GetAggregateComplianceDetailsByConfigRule",
            "config:DescribeConfigurationAggregators",
            "config:DescribeConfigurationAggregatorSourcesStatus",
            "config:DeleteConfigurationAggregator"
        ],
        "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-
aggregator-pokxzldx"
        }
    ]
}
```

接下来，用户确认 IAM 策略可用于限制对特定聚合器和规则的访问。

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-id AccountID
 --aws-region AwsRegion
```

该命令返回拒绝访问异常：

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User: arn:aws:iam::AccountID:user/ is
 not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

通过资源级权限，您可以授予或拒绝对多账户多区域数据聚合执行特定操作的访问权限。

附加信息

要了解有关创建 IAM 用户、组、策略和权限的更多信息，请参阅 IAM 用户指南中的创建您的第一个 IAM 用户和管理员组和访问控制。

Amazon Config Rules API 操作支持的资源级权限

资源级权限意指指定允许用户对哪些资源执行操作的功能。Amazon Config 支持某些 Amazon Config Rules API 操作的资源级权限。这意味着对于某些 Amazon Config Rules 操作，您可以控制何时允许用户执行操作 (基于必须满足的条件)或是允许用户使用的特定资源。

下表介绍当前支持资源级权限的 Amazon Config Rules API 操作，以及每个操作支持的资源（及其 ARN）。指定 ARN 时，您可以在路径中使用 * 通配符；例如，在无法或不希望指定确切资源 ID 的时候可以这样做。

Important

如果某一 Amazon Config Rules API 操作未在此表中列出，则表示它不支持资源级权限。如果 Amazon Config Rules 操作不支持资源级权限，您可以向用户授予使用该操作的权限，但必须为策略语句的资源元素指定 *。

API 操作	资源
DeleteConfigRule	Config 规则 arn:aws:config:*region:accountID*:config-rule/config-rule-*ID*
DeleteEvaluationResults	Config 规则 arn:aws:config:*region:accountID*:config-rule/config-rule-*ID*
DescribeComplianceByConfigRule	Config 规则 arn:aws:config:*region:accountID*:config-rule/config-rule-*ID*
DescribeConfigRuleEvaluationStatus	Config 规则 arn:aws:config:*region:accountID*:config-rule/config-rule-*ID*
DescribeConfigRules	Config 规则 arn:aws:config:*region:accountID*:config-rule/config-rule-*ID*
GetComplianceDetailsByConfigRule	Config 规则 arn:aws:config:*region:accountID*:config-rule/config-rule-*ID*
PutConfigRule	Config 规则 arn:aws:config:*region:accountID*:config-rule/config-rule-*ID*
StartConfigRulesEvaluation	Config 规则 arn:aws:config:*region:accountID*:config-rule/config-rule-*ID*
PutRemediationConfigurations	修复配置 arn:aws:config:*region:accountId*:remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationConfigurations	修复配置 arn:aws:config:*region:accountId*:remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationConfiguration	修复配置 arn:aws:config:*region:accountId*:remediation-configuration/*config rule name/remediation configuration id*
PutRemediationExceptions	修复配置

API 操作	资源
	arn:aws:config:*region:accountId*:remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediationExceptions	修复配置 arn:aws:config:*region:accountId*:remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediationExceptions	修复配置 arn:aws:config:*region:accountId*:remediation-configuration/*config rule name/remediation configuration id*

例如，您希望允许特定用户对特定规则进行的读访问，但拒绝特定用户对特定规则进行的写访问。

在第一个策略中，您允许 Amazon Config Rules 对指定规则进行读取操作，例如 `DescribeConfigRules` 和 `DescribeConfigRuleEvaluationStatus`。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:DescribeConfigRules",
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

在第二个策略中，您拒绝 Amazon Config Rules 对特定规则进行的写入操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
   }
```

利用资源级权限，您可以允许读取访问权限并拒绝写入访问权限以对 Amazon Config Rules API 操作执行特定操作。

服务相关联Amazon ConfigRule

服务相关的Amazon Configrule 是一种独特类型的托管配置规则Amazon要创建的服务Amazon Config您的账户中的规则。服务相关的Amazon Config规则已预定义以包含调用其他用户所需的所有权限Amazon代表您提供的服务。这些规则类似于Amazon服务推荐在你的Amazon Web Services 账户用于合规性验例：

这些服务相关的Amazon Config规则归属于Amazon服务团队。这些区域有：Amazon服务团队会在您的Amazon Web Services 账户. 您具有对这些规则的只读访问权限。如果您已订阅Amazon这些规则链接到的服务。

在 Amazon Config 控制台中，服务相关的 Amazon Config 规则将显示在 Rules (规则) 页面中。编辑按钮在控制台中将灰显，从而限制您编辑规则。您可以通过选择规则来查看规则的详细信息。在规则详细信息页面上，您可以查看已创建规则的服务的名称。Edit (编辑) 和 Delete results (删除结果) 将灰显，从而限制您编辑和删除规则的结果。要编辑或删除规则，请联系Amazon创建规则的服务。

在使用 Amazon Command Line Interface 时，`PutConfigRule`、`DeleteConfigRule` 和 `DeleteEvaluationResults` API 指示访问被拒绝，并显示以下错误消息：

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns ServiceLinkedConfigRule.
You do not have permissions to take action on this rule."
```

主题

- 对 Amazon Config 使用服务相关角色 (p. 235)

对 Amazon Config 使用服务相关角色

Amazon Config 使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与 Amazon Config 直接相关。服务相关角色由 Amazon Config 预定义，并包含该服务代表您调用其他 Amazon 服务所需的一切权限。

服务相关角色使 Amazon Config 的设置更轻松，因为您不必手动添加必要的权限。Amazon Config 定义其服务相关角色的权限，除非另行定义，否则仅 Amazon Config 可以代入其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其它 IAM 实体的权限策略。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的 Amazon 服务并查找 Service-Linked Role（服务相关角色）列中显示为 Yes（是）的服务。请选择 Yes 与查看该服务的服务相关角色文档的链接。

适用于 Amazon Config 的服务相关角色权限

Amazon Config使用名为 的服务相关角色。AWSServiceRoleForConfig–Amazon Config使用此服务相关角色来调用 otherAmazon代表您服务。

AWSServiceRoleForConfig 服务相关角色信任 `config.amazonaws.com` 服务来代入角色。

的权限策略`AWSServiceRoleForConfig`角色包含的只读权限和只写权限Amazon Config资源以及其他服务中资源的只读权限Amazon Config支持。有关更多信息，请参阅 支持的资源类型 (p. 7)。

必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅 IAM 用户指南中的服务相关角色权限。

将服务相关角色与Amazon Config，您必须配置针对 Amazon S3 存储桶和 Amazon SNS 主题的权限。有关更多信息，请参阅 使用服务相关角色时的 Amazon S3 存储桶的必需权限 (p. 222) 和 使用服务相关角色时 Amazon SNS 主题的必需权限 (p. 226)。

为 Amazon Config 创建服务相关角色

在 IAM CLI 或 IAM API 中，用 `config.amazonaws.com` 服务名称创建一个服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。如果您删除了此服务相关角色，则可以使用此相同过程再次创建角色。

编辑 Amazon Config 的服务相关角色

Amazon Config 不允许您编辑 AWSServiceRoleForConfig 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是可以使用 IAM 编辑角色说明。有关更多信息，请参见《IAM 用户指南》中的编辑服务相关角色。

删除 Amazon Config 的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果在您试图删除资源时 Amazon Config 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

要删除Amazon Config使用的资源AWSServiceRoleForConfig

确保您没有使用服务相关角色的 `ConfigurationRecorders`。您可以使用 Amazon Config 控制台停止配置记录器。要停止记录，请选择 Recording is on (记录已打开) 下的 Turn off (关闭)。

您可以使用 Amazon Config API 删除 `ConfigurationRecorder`。要删除，请使用 `delete-configuration-recorder` 命令。

```
        $ aws configservice delete-configuration-recorder --configuration-recorder-
name default
```

使用 IAM 手动删除服务相关角色

使用 IAM 控制台、IAM CLI 或 IAM API 删除 AWSServiceRoleForConfig 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适用于 Amazon Config 的托管策略

要向用户、组和角色添加权限，与自己编写策略相比，使用 Amazon 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。要快速入门，您可以使用我们的 Amazon 托管式策略。这些策略涵盖常见使用案例，可在您的 Amazon Web Services 账户 中使用。有关 Amazon 托管式策略的更多信息，请参阅 IAM 用户指南中的Amazon 托管式策略。

Amazon Web Services 负责维护和更新 Amazon 托管式策略。您无法更改 Amazon 托管式策略中的权限。服务偶尔会向 Amazon 托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 Amazon 托管式策略。服务不会从 Amazon 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，Amazon 还支持跨多种服务的工作职能的托管式策略。例如，`ViewOnlyAccess` Amazon 托管式策略提供对许多 Amazon Web Services 服务和资源的只读访问权限。当服务启动新功能时，Amazon 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 Amazon 托管策略。

Amazon管理的策略： AWSConfigServiceRolePolicy

Amazon Config使用名为 的服务相关角色。AWSServiceRoleForConfig打电话给其他人Amazon代表您服务。当您使用使用以下应用程序时：Amazon要设置的管理控制台Amazon Config，此单反相机由自动创建Amazon Config如果你选择该选项来使用Amazon ConfigSLR 而不是你自己的Amazon Identity and Access Management(IAM) 服务角色。

这些区域有：AWSServiceRoleForConfigSLR 包含托管策略`AWSConfigServiceRolePolicy`. 只只只只只只只只只只只只只只只只只只只只只只只只只只只只Amazon Config资源以及其他服务中资源的只读权限Amazon Config支持。有关更多信息，请参阅 支持的资源类型 (p. 7) 和 对 Amazon Config 使用服务相关角色 (p. 235)。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "access-analyzer:GetAnalyzer",
    "access-analyzer:GetArchiveRule",
    "access-analyzer:ListAnalyzers",
    "access-analyzer:ListArchiveRules",
    "access-analyzer:ListTagsForResource",
    "account:GetAlternateContact",
    "acm:DescribeCertificate",
    "acm:ListCertificates",
    "acm:ListTagsForCertificate",
    "amplifyuibuilder:GetTheme",
    "amplifyuibuilder:ExportThemes",
    "apigateway:GET",
    "appconfig:GetApplication",
    "appconfig:GetConfigurationProfile",
    "appconfig:GetDeployment",
    "appconfig:GetDeploymentStrategy",
    "appconfig:GetEnvironment",
    "appconfig:GetHostedConfigurationVersion",
    "appconfig:ListTagsForResource",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingPolicies",
    "appsync:GetGraphqlApi",
    "appsync:ListGraphqlApis",
    "athena:GetDataCatalog",
    "athena:GetWorkGroup",
    "athena:ListDataCatalogs",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeLifecycleHooks",
    "autoscaling:DescribePolicies",
    "autoscaling:DescribeScheduledActions",
    "autoscaling:DescribeTags",
    "backup-gateway:ListTagsForResource",
    "backup-gateway:ListVirtualMachines",
    "backup:DescribeBackupVault",
    "backup:DescribeRecoveryPoint",
    "backup:GetBackupPlan",
    "backup:GetBackupSelection",
    "backup:GetBackupVaultAccessPolicy",
    "backup:GetBackupVaultNotifications",
    "backup:ListBackupPlans",
    "backup:ListBackupSelections",
    "backup:ListBackupVaults",
    "backup:ListRecoveryPointsByBackupVault",
```

```
    "backup:ListTags",
    "batch:DescribeComputeEnvironments",
    "batch:DescribeJobQueues",
    "batch:ListTagsForResource",
    "billingconductor:ListBillingGroups",
    "billingconductor:ListAccountAssociations",
    "billingconductor:ListTagsForResource",
    "billingconductor:ListPricingRules",
    "billingconductor:ListCustomLineItems",
    "billingconductor:ListPricingPlans",
    "billingconductor:ListPricingRulesAssociatedToPricingPlan",
    "cloudformation:DescribeType",
    "cloudformation:GetResource",
    "cloudformation:ListResources",
    "cloudformation:ListTypes",
    "cloudfront:ListDistributions",
    "cloudfront:ListTagsForResource",
    "cloudtrail:DescribeTrails",
    "cloudtrail:GetEventDataStore",
    "cloudtrail:GetEventSelectors",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:ListEventDataStores",
    "cloudtrail:ListTags",
    "cloudwatch:DescribeAlarms",
    "codedeploy:GetDeploymentConfig",
    "codepipeline:GetPipeline",
    "codepipeline:GetPipelineState",
    "codepipeline:ListPipelines",
    "config:BatchGet*",
    "config:Describe*",
    "config:Get*",
    "config:List*",
    "config:Put*",
    "config:Select*",
    "datasync:DescribeAgent",
    "datasync:DescribeLocationEfs",
    "datasync:DescribeLocationFsxLustre",
    "datasync:DescribeLocationHdfs",
    "datasync:DescribeLocationNfs",
    "datasync:DescribeLocationObjectStorage",
    "datasync:DescribeLocationS3",
    "datasync:DescribeLocationSmb",
    "datasync:DescribeTask",
    "datasync:ListTagsForResource",
    "dax:DescribeClusters",
    "dax:DescribeParameterGroups",
    "dax:DescribeParameters",
    "dax:DescribeSubnetGroups",
    "dax:ListTags",
    "detective:ListGraphs",
    "detective:ListTagsForResource",
    "dms:DescribeCertificates",
    "dms:DescribeEventSubscriptions",
    "dms:DescribeReplicationInstances",
    "dms:DescribeReplicationSubnetGroups",
    "dms:DescribeReplicationTasks",
    "dms:ListTagsForResource",
    "dynamodb:DescribeContinuousBackups",
    "dynamodb:DescribeGlobalTable",
    "dynamodb:DescribeGlobalTableSettings",
    "dynamodb:DescribeLimits",
    "dynamodb:DescribeTable",
    "dynamodb:ListTables",
    "dynamodb:ListTagsOfResource",
    "ec2:Describe*",
    "ec2:DescribeClientVpnAuthorizationRules",
```

```
    "ec2:DescribeClientVpnEndpoints",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeFleets",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeSpotFleetRequests",
    "ec2:DescribeVolumeAttribute",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ecr-public:DescribeRepositories",
    "ecr-public:GetRepositoryCatalogData",
    "ecr-public:GetRepositoryPolicy",
    "ecr-public:ListTagsForResource",
    "ecr:DescribeRepositories",
    "ecr:DescribePullThroughCacheRules",
    "ecr:DescribeRegistry",
    "ecr:GetLifecyclePolicy",
    "ecr:GetRegistryPolicy",
    "ecr:GetRepositoryPolicy",
    "ecr:ListTagsForResource",
    "ecs:DescribeClusters",
    "ecs:DescribeServices",
    "ecs:DescribeTaskDefinition",
    "ecs:DescribeTaskSets",
    "ecs:ListClusters",
    "ecs:ListServices",
    "ecs:ListTagsForResource",
    "ecs:ListTaskDefinitionFamilies",
    "ecs:ListTaskDefinitions",
    "eks:DescribeCluster",
    "eks:DescribeFargateProfile",
    "eks:DescribeNodegroup",
    "eks:ListClusters",
    "eks:ListFargateProfiles",
    "eks:ListNodegroups",
    "eks:ListTagsForResource",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeCacheParameterGroups",
    "elasticache:DescribeCacheParameters",
    "elasticache:DescribeCacheSubnetGroups",
    "elasticache:DescribeReplicationGroups",
    "elasticache:DescribeSnapshots",
    "elasticache:ListTagsForResource",
    "elasticbeanstalk:DescribeConfigurationSettings",
    "elasticbeanstalk:DescribeEnvironments",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeBackupPolicy",
    "elasticfilesystem:DescribeFileSystemPolicy",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeLifecycleConfiguration",
    "elasticfilesystem:DescribeMountTargets",
    "elasticfilesystem:DescribeMountTargetSecurityGroups",
    "elasticloadbalancing:DescribeListenerCertificates",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancerPolicies",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:DescribeSecurityConfiguration",
    "elasticmapreduce:DescribeStep",
    "elasticmapreduce:GetBlockPublicAccessConfiguration",
```

```
    "elasticmapreduce:GetManagedScalingPolicy",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListInstanceFleets",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListInstances",
    "elasticmapreduce:ListSecurityConfigurations",
    "elasticmapreduce:ListSteps",
    "es:DescribeDomain",
    "es:DescribeDomains",
    "es:DescribeElasticsearchDomain",
    "es:DescribeElasticsearchDomains",
    "es:GetCompatibleElasticsearchVersions",
    "es:GetCompatibleVersions",
    "es:ListDomainNames",
    "es:ListTags",
    "events:DescribeArchive",
    "events:DescribeApiDestination",
    "firehose:DescribeDeliveryStream",
    "firehose:ListDeliveryStreams",
    "firehose:ListTagsForDeliveryStream",
    "fms:ListPolicies",
    "fms:GetPolicy",
    "fms:ListTagsForResource",
    "fms:GetNotificationChannel",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "fsx:ListTagsForResource",
    "geo:DescribeTracker",
    "geo:ListTrackerConsumers",
    "geo:DescribeGeofenceCollection",
    "geo:DescribePlaceIndex",
    "geo:DescribeRouteCalculator",
    "geo:DescribeMap",
    "globalaccelerator:DescribeAccelerator",
    "globalaccelerator:DescribeEndpointGroup",
    "globalaccelerator:DescribeListener",
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners",
    "globalaccelerator:ListTagsForResource",
    "glue:BatchGetDevEndpoints",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:GetCrawler",
    "glue:GetCrawlers",
    "glue:GetDevEndpoint",
    "glue:GetDevEndpoints",
    "glue:GetJob",
    "glue:GetJobs",
    "glue:GetSecurityConfiguration",
    "glue:GetSecurityConfigurations",
    "glue:GetTags",
    "glue:GetWorkflow",
    "glue:ListCrawlers",
    "glue:ListDevEndpoints",
    "glue:ListJobs",
    "glue:ListWorkflows",
    "guardduty:GetDetector",
    "guardduty:GetFilter",
    "guardduty:GetFindings",
    "guardduty:GetIPSet",
    "guardduty:GetMasterAccount",
    "guardduty:GetMembers",
    "guardduty:GetThreatIntelSet",
    "guardduty:ListDetectors",
    "guardduty:ListFilters",
```

```
    "guardduty:ListFindings",
    "guardduty:ListIPSets",
    "guardduty:ListMembers",
    "guardduty:ListOrganizationAdminAccounts",
    "guardduty:ListTagsForResource",
    "guardduty:ListThreatIntelSets",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
    "iam:GetGroup",
    "iam:GetGroupPolicy",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetUserPolicy",
    "iam:ListAttachedGroupPolicies",
    "iam:ListAttachedRolePolicies",
    "iam:ListAttachedUserPolicies",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroupsForUser",
    "iam:ListInstanceProfilesForRole",
    "iam:ListPolicyVersions",
    "iam:ListRolePolicies",
    "iam:ListUserPolicies",
    "iam:ListVirtualMFADevices",
    "imagebuilder:GetComponent",
    "imagebuilder:GetDistributionConfiguration",
    "imagebuilder:GetInfrastructureConfiguration",
    "imagebuilder:ListComponentBuildVersions",
    "imagebuilder:ListComponents",
    "imagebuilder:ListDistributionConfigurations",
    "imagebuilder:ListInfrastructureConfigurations",
    "kafka:DescribeCluster",
    "kafka:DescribeClusterV2",
    "kafka:ListClusters",
    "kafka:ListClustersV2",
    "kinesis:DescribeStreamConsumer",
    "kinesis:DescribeStreamSummary",
    "kinesis:ListStreamConsumers",
    "kinesis:ListStreams",
    "kinesis:ListTagsForStream",
    "kinesisanalytics:DescribeApplication",
    "kinesisanalytics:ListTagsForResource",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListAliases",
    "kms:ListKeys",
    "kms:ListResourceTags",
    "lambda:GetAlias",
    "lambda:GetFunction",
    "lambda:GetFunctionCodeSigningConfig",
    "lambda:GetPolicy",
    "lambda:ListAliases",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction",
    "logs:DescribeLogGroups",
    "logs:ListTagsLogGroup",
    "macie2:GetMacieSession",
    "network-firewall:DescribeLoggingConfiguration",
    "network-firewall:ListFirewalls",
```

```
    "opsworks:DescribeLayers",
    "opsworks:ListTags",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "organizations:ListParents",
    "organizations:ListPolicies",
    "organizations:ListPoliciesForTarget",
    "quicksight:DescribeDataSource",
    "quicksight:DescribeDataSourcePermissions",
    "quicksight:ListTagsForResource",
    "ram:GetResourceShareAssociations",
    "ram:GetResourceShares",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBClusters",
    "rds:DescribeDBClusterSnapshotAttributes",
    "rds:DescribeDBClusterSnapshots",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeDBParameterGroups",
    "rds:DescribeDBParameters",
    "rds:DescribeDBSecurityGroups",
    "rds:DescribeDBSnapshotAttributes",
    "rds:DescribeDBSnapshots",
    "rds:DescribeDBSubnetGroups",
    "rds:DescribeEventSubscriptions",
    "rds:DescribeOptionGroups",
    "rds:ListTagsForResource",
    "redshift:DescribeClusterParameterGroups",
    "redshift:DescribeClusterParameters",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSecurityGroups",
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeClusterSubnetGroups",
    "redshift:DescribeEventSubscriptions",
    "redshift:DescribeLoggingStatus",
    "rekognition:DescribeStreamProcessor",
    "rekognition:ListTagsForResource",
    "robomaker:DescribeRobotApplication",
    "robomaker:DescribeSimulationApplication",
    "route53:GetHealthCheck",
    "route53:GetHostedZone",
    "route53:ListHealthChecks",
    "route53:ListHostedZones",
    "route53:ListHostedZonesByName",
    "route53:ListQueryLoggingConfigs",
    "route53:ListResourceRecordSets",
    "route53:ListTagsForResource",
    "route53resolver:GetResolverEndpoint",
    "route53resolver:GetResolverRule",
    "route53resolver:GetResolverRuleAssociation",
    "route53resolver:ListResolverEndpointIpAddresses",
    "route53resolver:ListResolverEndpoints",
    "route53resolver:ListResolverRuleAssociations",
    "route53resolver:ListResolverRules",
    "route53resolver:ListTagsForResource",
    "s3:GetAccelerateConfiguration",
    "s3:GetAccessPoint",
    "s3:GetAccessPointPolicy",
    "s3:GetAccessPointPolicyStatus",
    "s3:GetAccountPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketCORS",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketNotification",
```

```
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketRequestPayment",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:GetStorageLensConfiguration",
    "s3:GetStorageLensConfigurationTagging",
    "s3:ListAccessPoints",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "sagemaker:DescribeCodeRepository",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:DescribeModel",
    "sagemaker:DescribeMonitoringSchedule",
    "sagemaker:DescribeNotebookInstance",
    "sagemaker:DescribeNotebookInstanceLifecycleConfig",
    "sagemaker:DescribeWorkteam",
    "sagemaker:ListCodeRepositories",
    "sagemaker:ListEndpointConfigs",
    "sagemaker:ListEndpoints",
    "sagemaker:ListModels",
    "sagemaker:ListMonitoringSchedules",
    "sagemaker:ListNotebookInstanceLifecycleConfigs",
    "sagemaker:ListNotebookInstances",
    "sagemaker:ListTags",
    "sagemaker:ListWorkteams",
    "secretsmanager:ListSecrets",
    "secretsmanager:ListSecretVersionIds",
    "securityhub:DescribeHub",
    "servicediscovery:GetInstance",
    "servicediscovery:GetNamespace",
    "servicediscovery:GetService",
    "servicediscovery:ListTagsForResource",
    "ses:DescribeReceiptRule",
    "ses:DescribeReceiptRuleSet",
    "ses:GetConfigurationSet",
    "ses:GetConfigurationSetEventDestinations",
    "ses:GetContactList",
    "ses:GetEmailTemplate",
    "ses:GetTemplate",
    "ses:ListConfigurationSets",
    "shield:DescribeDRTAccess",
    "shield:DescribeProtection",
    "shield:DescribeSubscription",
    "sns:GetSubscriptionAttributes",
    "sns:GetTopicAttributes",
    "sns:ListSubscriptions",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTagsForResource",
    "sns:ListTopics",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues",
    "sqs:ListQueueTags",
    "ssm:DescribeAutomationExecutions",
    "ssm:DescribeDocument",
    "ssm:DescribeDocumentPermission",
    "ssm:GetAutomationExecution",
    "ssm:GetDocument",
    "ssm:ListDocuments",
    "sso:DescribeInstanceAccessControlAttributeConfiguration",
```

```
    "sso:DescribePermissionSet",
    "sso:GetInlinePolicyForPermissionSet",
    "sso:ListManagedPoliciesInPermissionSet",
    "sso:ListPermissionSets",
    "sso:ListTagsForResource",
    "states:DescribeActivity",
    "states:DescribeStateMachine",
    "states:ListActivities",
    "states:ListStateMachines",
    "states:ListTagsForResource",
    "storagegateway:ListGateways",
    "storagegateway:ListTagsForResource",
    "storagegateway:ListVolumes",
    "support:DescribeCases",
    "tag:GetResources",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:GetWebACL",
    "waf-regional:GetWebACLForResource",
    "waf:GetLoggingConfiguration",
    "waf:GetWebACL",
    "wafv2:GetLoggingConfiguration",
    "wafv2:GetRuleGroup",
    "wafv2:ListRuleGroups",
    "wafv2:ListTagsForResource",
    "workspaces:DescribeConnectionAliases",
    "workspaces:DescribeTags",
    "workspaces:DescribeWorkspaces"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogStream",
    "logs:CreateLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/config/*"
  },
  {
   "Effect": "Allow",
   "Action": "logs:PutLogEvents",
   "Resource": "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-evaluation/
*"
  }
 ]
}
```

Amazon管理的策略：AWS_ConfigRole

录制你的Amazon资源配置，Amazon Config需要 IAM 权限才能获取有关您的资源的配置详细信息。如果您要为创建 IAM 角色Amazon Config，您可以使用托管策略`AWS_ConfigRole`并将其附加到您的 IAM 角色。

此 IAM 策略每次都会更新Amazon Config添加了对以下应用程序的支持：Amazon资源类型。这意味着Amazon Config将继续拥有记录受支持资源类型的配置数据所需的权限，只要AWS_ConfigRole角色附加了此托管策略。有关更多信息，请参阅 支持的资源类型 (p. 7) 和 分配给的 IAM 角色权限Amazon Config (p. 218)。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
```

```
    "access-analyzer:GetAnalyzer",
    "access-analyzer:GetArchiveRule",
    "access-analyzer:ListAnalyzers",
    "access-analyzer:ListArchiveRules",
    "access-analyzer:ListTagsForResource",
    "account:GetAlternateContact",
    "acm:DescribeCertificate",
    "acm:ListCertificates",
    "acm:ListTagsForCertificate",
    "amplifyuibuilder:GetTheme",
    "amplifyuibuilder:ExportThemes",
    "apigateway:GET",
    "appconfig:GetApplication",
    "appconfig:GetConfigurationProfile",
    "appconfig:GetDeployment",
    "appconfig:GetDeploymentStrategy",
    "appconfig:GetEnvironment",
    "appconfig:GetHostedConfigurationVersion",
    "appconfig:ListTagsForResource",
    "application-autoscaling:DescribeScalableTargets",
    "application-autoscaling:DescribeScalingPolicies",
    "appsync:GetGraphqlApi",
    "appsync:ListGraphqlApis",
    "athena:GetDataCatalog",
    "athena:GetWorkGroup",
    "athena:ListDataCatalogs",
    "athena:ListTagsForResource",
    "athena:ListWorkGroups",
    "autoscaling:DescribeAutoScalingGroups",
    "autoscaling:DescribeLaunchConfigurations",
    "autoscaling:DescribeLifecycleHooks",
    "autoscaling:DescribePolicies",
    "autoscaling:DescribeScheduledActions",
    "autoscaling:DescribeTags",
    "backup-gateway:ListTagsForResource",
    "backup-gateway:ListVirtualMachines",
    "backup:DescribeBackupVault",
    "backup:DescribeRecoveryPoint",
    "backup:GetBackupPlan",
    "backup:GetBackupSelection",
    "backup:GetBackupVaultAccessPolicy",
    "backup:GetBackupVaultNotifications",
    "backup:ListBackupPlans",
    "backup:ListBackupSelections",
    "backup:ListBackupVaults",
    "backup:ListRecoveryPointsByBackupVault",
    "backup:ListTags",
    "batch:DescribeComputeEnvironments",
    "batch:DescribeJobQueues",
    "batch:ListTagsForResource",
    "billingconductor:ListBillingGroups",
    "billingconductor:ListAccountAssociations",
    "billingconductor:ListTagsForResource",
    "billingconductor:ListPricingRules",
    "billingconductor:ListCustomLineItems",
    "billingconductor:ListPricingPlans",
    "billingconductor:ListPricingRulesAssociatedToPricingPlan",
    "cloudformation:DescribeType",
    "cloudformation:GetResource",
    "cloudformation:ListResources",
    "cloudformation:ListTypes",
    "cloudfront:ListDistributions",
    "cloudfront:ListTagsForResource",
    "cloudtrail:DescribeTrails",
    "cloudtrail:GetEventDataStore",
    "cloudtrail:GetEventSelectors",
```

```
    "cloudtrail:GetTrailStatus",
    "cloudtrail:ListEventDataStores",
    "cloudtrail:ListTags",
    "cloudwatch:DescribeAlarms",
    "codedeploy:GetDeploymentConfig",
    "codepipeline:GetPipeline",
    "codepipeline:GetPipelineState",
    "codepipeline:ListPipelines",
    "config:BatchGet*",
    "config:Describe*",
    "config:Get*",
    "config:List*",
    "config:Put*",
    "config:Select*",
    "datasync:DescribeAgent",
    "datasync:DescribeLocationEfs",
    "datasync:DescribeLocationFsxLustre",
    "datasync:DescribeLocationHdfs",
    "datasync:DescribeLocationNfs",
    "datasync:DescribeLocationObjectStorage",
    "datasync:DescribeLocationS3",
    "datasync:DescribeLocationSmb",
    "datasync:DescribeTask",
    "datasync:ListTagsForResource",
    "dax:DescribeClusters",
    "dax:DescribeParameterGroups",
    "dax:DescribeParameters",
    "dax:DescribeSubnetGroups",
    "dax:ListTags",
    "detective:ListGraphs",
    "detective:ListTagsForResource",
    "dms:DescribeCertificates",
    "dms:DescribeEventSubscriptions",
    "dms:DescribeReplicationInstances",
    "dms:DescribeReplicationSubnetGroups",
    "dms:DescribeReplicationTasks",
    "dms:ListTagsForResource",
    "dynamodb:DescribeContinuousBackups",
    "dynamodb:DescribeGlobalTable",
    "dynamodb:DescribeGlobalTableSettings",
    "dynamodb:DescribeLimits",
    "dynamodb:DescribeTable",
    "dynamodb:ListTables",
    "dynamodb:ListTagsOfResource",
    "ec2:Describe*",
    "ec2:DescribeClientVpnAuthorizationRules",
    "ec2:DescribeClientVpnEndpoints",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeFleets",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeSpotFleetRequests",
    "ec2:DescribeVolumeAttribute",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ecr-public:DescribeRepositories",
    "ecr-public:GetRepositoryCatalogData",
    "ecr-public:GetRepositoryPolicy",
    "ecr-public:ListTagsForResource",
    "ecr:DescribeRepositories",
    "ecr:DescribePullThroughCacheRules",
    "ecr:DescribeRegistry",
    "ecr:GetLifecyclePolicy",
    "ecr:GetRegistryPolicy",
    "ecr:GetRepositoryPolicy",
    "ecr:ListTagsForResource",
```

```
    "ecs:DescribeClusters",
    "ecs:DescribeServices",
    "ecs:DescribeTaskDefinition",
    "ecs:DescribeTaskSets",
    "ecs:ListClusters",
    "ecs:ListServices",
    "ecs:ListTagsForResource",
    "ecs:ListTaskDefinitionFamilies",
    "ecs:ListTaskDefinitions",
    "eks:DescribeCluster",
    "eks:DescribeFargateProfile",
    "eks:DescribeNodegroup",
    "eks:ListClusters",
    "eks:ListFargateProfiles",
    "eks:ListNodegroups",
    "eks:ListTagsForResource",
    "elasticache:DescribeCacheClusters",
    "elasticache:DescribeCacheParameterGroups",
    "elasticache:DescribeCacheParameters",
    "elasticache:DescribeCacheSubnetGroups",
    "elasticache:DescribeReplicationGroups",
    "elasticache:DescribeSnapshots",
    "elasticache:ListTagsForResource",
    "elasticbeanstalk:DescribeConfigurationSettings",
    "elasticbeanstalk:DescribeEnvironments",
    "elasticfilesystem:DescribeAccessPoints",
    "elasticfilesystem:DescribeBackupPolicy",
    "elasticfilesystem:DescribeFileSystemPolicy",
    "elasticfilesystem:DescribeFileSystems",
    "elasticfilesystem:DescribeLifecycleConfiguration",
    "elasticfilesystem:DescribeMountTargets",
    "elasticfilesystem:DescribeMountTargetSecurityGroups",
    "elasticloadbalancing:DescribeListenerCertificates",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancerPolicies",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetHealth",
    "elasticmapreduce:DescribeCluster",
    "elasticmapreduce:DescribeSecurityConfiguration",
    "elasticmapreduce:DescribeStep",
    "elasticmapreduce:GetBlockPublicAccessConfiguration",
    "elasticmapreduce:GetManagedScalingPolicy",
    "elasticmapreduce:ListClusters",
    "elasticmapreduce:ListInstanceFleets",
    "elasticmapreduce:ListInstanceGroups",
    "elasticmapreduce:ListInstances",
    "elasticmapreduce:ListSecurityConfigurations",
    "elasticmapreduce:ListSteps",
    "es:DescribeDomain",
    "es:DescribeDomains",
    "es:DescribeElasticsearchDomain",
    "es:DescribeElasticsearchDomains",
    "es:GetCompatibleElasticsearchVersions",
    "es:GetCompatibleVersions",
    "es:ListDomainNames",
    "es:ListTags",
    "events:DescribeArchive",
    "events:DescribeApiDestination",
    "firehose:DescribeDeliveryStream",
    "firehose:ListDeliveryStreams",
    "firehose:ListTagsForDeliveryStream",
```

```
    "fms:ListPolicies",
    "fms:GetPolicy",
    "fms:ListTagsForResource",
    "fms:GetNotificationChannel",
    "fsx:DescribeFileSystems",
    "fsx:DescribeVolumes",
    "fsx:ListTagsForResource",
    "geo:DescribeTracker",
    "geo:ListTrackerConsumers",
    "geo:DescribeGeofenceCollection",
    "geo:DescribePlaceIndex",
    "geo:DescribeRouteCalculator",
    "geo:DescribeMap",
    "globalaccelerator:DescribeAccelerator",
    "globalaccelerator:DescribeEndpointGroup",
    "globalaccelerator:DescribeListener",
    "globalaccelerator:ListAccelerators",
    "globalaccelerator:ListEndpointGroups",
    "globalaccelerator:ListListeners",
    "globalaccelerator:ListTagsForResource",
    "glue:BatchGetDevEndpoints",
    "glue:BatchGetJobs",
    "glue:BatchGetWorkflows",
    "glue:GetCrawler",
    "glue:GetCrawlers",
    "glue:GetDevEndpoint",
    "glue:GetDevEndpoints",
    "glue:GetJob",
    "glue:GetJobs",
    "glue:GetSecurityConfiguration",
    "glue:GetSecurityConfigurations",
    "glue:GetTags",
    "glue:GetWorkflow",
    "glue:ListCrawlers",
    "glue:ListDevEndpoints",
    "glue:ListJobs",
    "glue:ListWorkflows",
    "guardduty:GetDetector",
    "guardduty:GetFilter",
    "guardduty:GetFindings",
    "guardduty:GetIPSet",
    "guardduty:GetMasterAccount",
    "guardduty:GetMembers",
    "guardduty:GetThreatIntelSet",
    "guardduty:ListDetectors",
    "guardduty:ListFilters",
    "guardduty:ListFindings",
    "guardduty:ListIPSets",
    "guardduty:ListMembers",
    "guardduty:ListOrganizationAdminAccounts",
    "guardduty:ListTagsForResource",
    "guardduty:ListThreatIntelSets",
    "iam:GenerateCredentialReport",
    "iam:GetAccountAuthorizationDetails",
    "iam:GetAccountPasswordPolicy",
    "iam:GetAccountSummary",
    "iam:GetCredentialReport",
    "iam:GetGroup",
    "iam:GetGroupPolicy",
    "iam:GetPolicy",
    "iam:GetPolicyVersion",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:GetUser",
    "iam:GetUserPolicy",
    "iam:ListAttachedGroupPolicies",
```

```
    "iam:ListAttachedRolePolicies",
    "iam:ListAttachedUserPolicies",
    "iam:ListEntitiesForPolicy",
    "iam:ListGroupPolicies",
    "iam:ListGroupsForUser",
    "iam:ListInstanceProfilesForRole",
    "iam:ListPolicyVersions",
    "iam:ListRolePolicies",
    "iam:ListUserPolicies",
    "iam:ListVirtualMFADevices",
    "imagebuilder:GetComponent",
    "imagebuilder:GetDistributionConfiguration",
    "imagebuilder:GetInfrastructureConfiguration",
    "imagebuilder:ListComponentBuildVersions",
    "imagebuilder:ListComponents",
    "imagebuilder:ListDistributionConfigurations",
    "imagebuilder:ListInfrastructureConfigurations",
    "kafka:DescribeCluster",
    "kafka:DescribeClusterV2",
    "kafka:ListClusters",
    "kafka:ListClustersV2",
    "kinesis:DescribeStreamConsumer",
    "kinesis:DescribeStreamSummary",
    "kinesis:ListStreamConsumers",
    "kinesis:ListStreams",
    "kinesis:ListTagsForStream",
    "kinesisanalytics:DescribeApplication",
    "kinesisanalytics:ListTagsForResource",
    "kms:DescribeKey",
    "kms:GetKeyPolicy",
    "kms:GetKeyRotationStatus",
    "kms:ListAliases",
    "kms:ListKeys",
    "kms:ListResourceTags",
    "lambda:GetAlias",
    "lambda:GetFunction",
    "lambda:GetFunctionCodeSigningConfig",
    "lambda:GetPolicy",
    "lambda:ListAliases",
    "lambda:ListFunctions",
    "lambda:ListVersionsByFunction",
    "logs:DescribeLogGroups",
    "logs:ListTagsLogGroup",
    "macie2:GetMacieSession",
    "network-firewall:DescribeLoggingConfiguration",
    "network-firewall:ListFirewalls",
    "opsworks:DescribeLayers",
    "opsworks:ListTags",
    "organizations:DescribeOrganization",
    "organizations:DescribePolicy",
    "organizations:ListParents",
    "organizations:ListPolicies",
    "organizations:ListPoliciesForTarget",
    "quicksight:DescribeDataSource",
    "quicksight:DescribeDataSourcePermissions",
    "quicksight:ListTagsForResource",
    "ram:GetResourceShareAssociations",
    "ram:GetResourceShares",
    "rds:DescribeDBClusterParameterGroups",
    "rds:DescribeDBClusterParameters",
    "rds:DescribeDBClusters",
    "rds:DescribeDBClusterSnapshotAttributes",
    "rds:DescribeDBClusterSnapshots",
    "rds:DescribeDBEngineVersions",
    "rds:DescribeDBInstances",
    "rds:DescribeDBParameterGroups",
```

```
    "rds:DescribeDBParameters",
    "rds:DescribeDBSecurityGroups",
    "rds:DescribeDBSnapshotAttributes",
    "rds:DescribeDBSnapshots",
    "rds:DescribeDBSubnetGroups",
    "rds:DescribeEventSubscriptions",
    "rds:DescribeOptionGroups",
    "rds:ListTagsForResource",
    "redshift:DescribeClusterParameterGroups",
    "redshift:DescribeClusterParameters",
    "redshift:DescribeClusters",
    "redshift:DescribeClusterSecurityGroups",
    "redshift:DescribeClusterSnapshots",
    "redshift:DescribeClusterSubnetGroups",
    "redshift:DescribeEventSubscriptions",
    "redshift:DescribeLoggingStatus",
    "rekognition:DescribeStreamProcessor",
    "rekognition:ListTagsForResource",
    "robomaker:DescribeRobotApplication",
    "robomaker:DescribeSimulationApplication",
    "route53:GetHealthCheck",
    "route53:GetHostedZone",
    "route53:ListHealthChecks",
    "route53:ListHostedZones",
    "route53:ListHostedZonesByName",
    "route53:ListQueryLoggingConfigs",
    "route53:ListResourceRecordSets",
    "route53:ListTagsForResource",
    "route53resolver:GetResolverEndpoint",
    "route53resolver:GetResolverRule",
    "route53resolver:GetResolverRuleAssociation",
    "route53resolver:ListResolverEndpointIpAddresses",
    "route53resolver:ListResolverEndpoints",
    "route53resolver:ListResolverRuleAssociations",
    "route53resolver:ListResolverRules",
    "route53resolver:ListTagsForResource",
    "s3:GetAccelerateConfiguration",
    "s3:GetAccessPoint",
    "s3:GetAccessPointPolicy",
    "s3:GetAccessPointPolicyStatus",
    "s3:GetAccountPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketCORS",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketNotification",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetBucketPolicy",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketRequestPayment",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetEncryptionConfiguration",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration",
    "s3:GetStorageLensConfiguration",
    "s3:GetStorageLensConfigurationTagging",
    "s3:ListAccessPoints",
    "s3:ListAllMyBuckets",
    "s3:ListBucket",
    "sagemaker:DescribeCodeRepository",
    "sagemaker:DescribeEndpoint",
    "sagemaker:DescribeEndpointConfig",
    "sagemaker:DescribeModel",
    "sagemaker:DescribeMonitoringSchedule",
```

```
    "sagemaker:DescribeNotebookInstance",
    "sagemaker:DescribeNotebookInstanceLifecycleConfig",
    "sagemaker:DescribeWorkteam",
    "sagemaker:ListCodeRepositories",
    "sagemaker:ListEndpointConfigs",
    "sagemaker:ListEndpoints",
    "sagemaker:ListModels",
    "sagemaker:ListMonitoringSchedules",
    "sagemaker:ListNotebookInstanceLifecycleConfigs",
    "sagemaker:ListNotebookInstances",
    "sagemaker:ListTags",
    "sagemaker:ListWorkteams",
    "secretsmanager:ListSecrets",
    "secretsmanager:ListSecretVersionIds",
    "securityhub:DescribeHub",
    "servicediscovery:GetInstance",
    "servicediscovery:GetNamespace",
    "servicediscovery:GetService",
    "servicediscovery:ListTagsForResource",
    "ses:DescribeReceiptRule",
    "ses:DescribeReceiptRuleSet",
    "ses:GetConfigurationSet",
    "ses:GetConfigurationSetEventDestinations",
    "ses:GetContactList",
    "ses:GetEmailTemplate",
    "ses:GetTemplate",
    "ses:ListConfigurationSets",
    "shield:DescribeDRTAccess",
    "shield:DescribeProtection",
    "shield:DescribeSubscription",
    "sns:GetSubscriptionAttributes",
    "sns:GetTopicAttributes",
    "sns:ListSubscriptions",
    "sns:ListSubscriptionsByTopic",
    "sns:ListTagsForResource",
    "sns:ListTopics",
    "sqs:GetQueueAttributes",
    "sqs:ListQueues",
    "sqs:ListQueueTags",
    "ssm:DescribeAutomationExecutions",
    "ssm:DescribeDocument",
    "ssm:DescribeDocumentPermission",
    "ssm:GetAutomationExecution",
    "ssm:GetDocument",
    "ssm:ListDocuments",
    "sso:DescribeInstanceAccessControlAttributeConfiguration",
    "sso:DescribePermissionSet",
    "sso:GetInlinePolicyForPermissionSet",
    "sso:ListManagedPoliciesInPermissionSet",
    "sso:ListPermissionSets",
    "sso:ListTagsForResource",
    "states:DescribeActivity",
    "states:DescribeStateMachine",
    "states:ListActivities",
    "states:ListStateMachines",
    "states:ListTagsForResource",
    "storagegateway:ListGateways",
    "storagegateway:ListTagsForResource",
    "storagegateway:ListVolumes",
    "support:DescribeCases",
    "tag:GetResources",
    "waf-regional:GetLoggingConfiguration",
    "waf-regional:GetWebACL",
    "waf-regional:GetWebACLForResource",
    "waf:GetLoggingConfiguration",
    "waf:GetWebACL",
```

```
    "wafv2:GetLoggingConfiguration",
    "wafv2:GetRuleGroup",
    "wafv2:ListRuleGroups",
    "wafv2:ListTagsForResource",
    "workspaces:DescribeConnectionAliases",
    "workspaces:DescribeTags",
    "workspaces:DescribeWorkspaces"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogStream",
    "logs:CreateLogGroup"
   ],
   "Resource": "arn:aws:logs:*:*:log-group:/aws/config/*"
  },
  {
   "Effect": "Allow",
   "Action": "logs:PutLogEvents",
   "Resource": "arn:aws:logs:*:*:log-group:/aws/config/*:log-stream:config-rule-evaluation/
*"
  }
 ]
}
```

对 Amazon 托管式策略的 Amazon Config 更新

查看有关 Amazon Config 的 Amazon 托管式策略更新的详细信息（从该服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅Amazon Config 文档历史记录页.

更改	说明	日期
AWSConfigServiceRolePolicy (p. 23)添加 amplifyuibuilder：ExportThemes，amplifyuibuilder：GetTheme，appconfig：GetApplication，appconfig：GetApplication，appconfig：GetConfigurationProfile，appconfig：GetConfigurationProfile，appconfig：GetDeployment，appconfig：GetDeploymentStrategy，appconfig：GetEnvironment，appconfig：GetHostedConfigurationVersion，appconfig：ListTagsForResource，appsond：GetGraphqlApi，appsond：ListGraphqlApis，billingconductor：ListPricingRulesAssociatedToPricingPlan，billingconductor：ListAccountAssociations，billingconductor：ListBillingGroups，billingconductor：ListCustomLineItems，billingconductor：ListPricingPlans，billingconductor：ListPricingRules，billingconductor：ListTagsForResource，数据同步：DescribeAgent，数据同步：DescribeLocationEfs，数据同步：	此策略现在支持的额外权限 Amazon Amplify、Amazon AppConfig、Amazon AppSync、AmazonConductorAmazon DataSync、Amazon Firewall Manager、Amazon Glue、Amazon IAM Identity Center (successor to Amazon Single Sign-On)(IAM Identity Center)、Amazon Elastic Container Service (Ama ElastiCache，Amazon EventBridge、亚马逊 FSX、Amazon Kinesis Data Analytics、亚马逊Location Service、亚马逊Managed Streaming for Apache Kafka、亚马逊 QuickSight、Amazon Rekognition、亚马逊 RoboMaker、Amazon Simple Storage Service (Amazon S3)、Amazon Simple Email Service (Amazon SES)、EC2	2022 年 7 月 15 日

更改	说明	日期
DescribeLocationFsxLustre，数据同步：DescribeLocationHdfs，数据同步：DescribeLocationNfs，数据同步：DescribeLocationObjectStorage，数据同步：DescribeLocationS3，数据同步：DescribeLocationSmb，数据同步：DescribeTask，数据同步：ListTagsForResource，ecr：DescribePullThroughCacheRules，ecr：DescribeRegistry，ecr：GetRegistryPolicy，elasticache:DescribeCacheParameters，弹性负载均衡：DescribeListenerCertificates，弹性负载均衡：DescribeTargetGroupAttributes，弹性负载均衡：DescribeTargetGroups，弹性负载均衡：DescribeTargetHealth，事件：DescribeApiDestination，事件：DescribeArchive，fms：GetNotificationChannel，fms：GetPolicy，fms：ListPolicies，fms：ListTagsForResource，fsx：DescribeVolumes，eoDescribeGeofenceCollection，eoDescribeMap，eoDescribePlaceIndex，eoDescribeRouteCalculator，eoDescribeTracker，eoListTrackerConsumers，glinke：BatchGetJobs，glinke：BatchGetWorkflows，glinke：GetCrawler，glinke：GetCrawlers，glinke：GetJob，glinke：GetJobs，glinke：GetWorkflow，imagebuilder：GetComponent，imagebuilder：ListComponentBuildVersions，imagebuilder：ListComponents，imagebuilder：GetDistributionConfiguration，imagebuilder：GetInfrastructureConfiguration，imagebuilder：ListDistributionConfigurations，imeBuilder：ListInfrastructureConfigurations，kafka：DescribeClusterV2，kafka：ListClustersV2，kinesisAnalytics：DescribeApplication，kinesisAnalytics：ListTagsForResource，quicksight：DescribeDataSource，quicksight：DescribeDataSourcePermissions，quicksight：ListTagsForResource，rekognition：		

更改	说明	日期
DescribeStreamProcessor，rekognition：ListTagsForResource，robomaker：DescribeRobotApplication，robomaker：DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging，服务发现：GetInstance，服务发现：GetNamespace，服务发现：GetService，服务发现：ListTagsForResource, 请参阅:DescribeReceiptRule, 请参阅:DescribeReceiptRuleSet, 请参阅:GetContactList, 请参阅:GetEmailTemplate, 请参阅:GetTemplate，等等：GetInlinePolicyForPermissionSet		

更改	说明	日期
AWS_ConfigRole (p. 244)—添加 amplifyuibuilder：ExportThemes，amplifyuibuilder：GetTheme，appconfig：GetApplication，appconfig：GetApplication，appconfig：GetConfigurationProfile，appconfig：GetConfigurationProfile，appconfig：GetDeployment，appconfig：GetDeploymentStrategy，appconfig：GetEnvironment，appconfig：GetHostedConfigurationVersion，appconfig：ListTagsForResource，appsond：GetGraphqlApi，appsond：ListGraphqlApis，billingconductor：ListPricingRulesAssociatedToPricingPlan，billingconductor：ListAccountAssociations，billingconductor：ListBillingGroups，billingconductor：ListCustomLineItems，billingconductor：ListPricingPlans，billingconductor：ListPricingRules，billingconductor：ListTagsForResource，数据同步：DescribeAgent，数据同步：DescribeLocationEfs，数据同步：DescribeLocationFsxLustre，数据同步：DescribeLocationHdfs，数据同步：DescribeLocationNfs，数据同步：DescribeLocationObjectStorage，数据同步：DescribeLocationS3，数据同步：DescribeLocationSmb，数据同步：DescribeTask，数据同步：ListTagsForResource，ecr：DescribePullThroughCacheRules，ecr：DescribeRegistry，ecr：GetRegistryPolicy，elasticache:DescribeCacheParameters，弹性负载均衡：DescribeListenerCertificates，弹性负载均衡：DescribeTargetGroupAttributes，弹性负载均衡：DescribeTargetGroups，弹性负载均衡：DescribeTargetHealth，事件：DescribeApiDestination，事件：DescribeArchive，fms：GetNotificationChannel，fms：GetPolicy，fms：ListPolicies，fms：ListTagsForResource，fsx：DescribeVolumes, eoDescribeGeofenceCollection, eoDescribeMap,	此策略现在支持的额外权限 Amazon Amplify、Amazon AppConfig、Amazon AppSync、AmazonConductorAmazon DataSync、Amazon Firewall Manager、Amazon Glue、Amazon IAM Identity Center (successor to Amazon Single Sign-On)(IAM Identity Center)、Amazon Elastic Container Service (Ama ElastiCache，Amazon EventBridge、亚马逊 FSX、Amazon Kinesis Data Analytics、亚马逊Location Service、Amazon Managed Streaming for Apache Kafka、亚马逊 QuickSight、Amazon Rekognition、亚马逊 RoboMaker、Amazon Simple Storage Service (Amazon S3)、Amazon Simple Email Service (Amazon SES)、EC2	2022 年 7 月 15 日

更改	说明	日期
eoDescribePlaceIndex, eoDescribeRouteCalculator, eoDescribeTracker, eoListTrackerConsumers，glinke：BatchGetJobs，glinke：BatchGetWorkflows，glinke：GetCrawler，glinke：GetCrawlers，glinke：GetJob，glinke：GetJobs，glinke：GetWorkflow，imagebuilder：GetComponent，imagebuilder：ListComponentBuildVersions，imagebuilder：ListComponents，imagebuilder：GetDistributionConfiguration，imagebuilder：GetInfrastructureConfiguration，imagebuilder：ListDistributionConfigurations，imagebuilder：ListInfrastructureConfigurations，kafka：DescribeClusterV2，kafka：ListClustersV2，kinesisAnalytics：DescribeApplication，kinesisAnalytics：ListTagsForResource，quicksight：DescribeDataSource，quicksight：DescribeDataSourcePermissions，quicksight：ListTagsForResource，rekognition：DescribeStreamProcessor，rekognition：ListTagsForResource，robomaker：DescribeRobotApplication，robomaker：DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging，服务发现：GetInstance，服务发现：GetNamespace，服务发现：GetService，服务发现：ListTagsForResource, 请参阅:DescribeReceiptRule, 请参阅:DescribeReceiptRuleSet, 请参阅:GetContactList, 请参阅:GetEmailTemplate, 请参阅:GetTemplate，等等：GetInlinePolicyForPermissionSet		

更改	说明	日期
AWSConfigServiceRolePolicy (p. 23) 添加雅典娜： GetDataCatalog，athena： ListDataCatalogs，athena： ListTagsForResource，detectiveListGraphs，detectiveListTagsForResource，glinke： BatchGetDevEndpoints，glinke： GetDevEndpoint，glinke： GetDevEndpoints，glinke： GetSecurityConfiguration，glinke： GetSecurityConfigurations，glinke： GetTags 粘 附:GetWorkGroup，glinke： ListCrawlers，glinke： ListDevEndpoints，glinke： ListJobs，glinke： ListMembers，glinke： ListWorkflows，glinke： ListWorkGroups，guarduty： GetFilter，警卫职责： getipset，警卫职责： GetThreatIntelSet，guarduty： GetMembers，guarduty： ListFilters，警卫职责： listipsets，警卫职责： ListTagsForResource，guarduty： ListThreatIntelSets，macie： GetMacieSession， ram:GetResourceShareAssociations， ram:GetResourceShares，请参阅:GetConfigurationSet，请参阅:GetConfigurationSetEventDestinations，请参阅:ListConfigurationSets， 所以： DescribeInstanceAccessControlAttributeConfiguration， 所以： DescribePermissionSet，所以： ListManagedPoliciesInPermissionSet， 所以：ListPermissionSets，等等：ListTagsForResource	此策略现在授予权限以获取指定的 Amazon Athena 数据目录，在Amazon账户，并列出与 Athena 工作组或数据目录资源关联的标签；获取 Amazon Detective 行为图表列表和 Detective 行为图的列表标签；获取给定列表的资源元数据列表Amazon Glue开发终端节点名称，获取有关指定终端节点的详细信息Amazon Glue开发端点，获取所有Amazon Glue开发终端节点位于Amazon账户，检索指定的Amazon Glue安全配置，全部获取Amazon Glue安全配置，获取与安全配置关联的标签列表Amazon Glue资源，获取有关的信息Amazon Glue具有指定名称的工作组，检索所有Amazon Glue爬虫资源位于Amazon账户，获取所有人的名字Amazon Glue `DevEndpoint`资源在Amazon账户，列出所有账户Amazon Glue中的任务资源Amazon账户，获取有关的详细信息Amazon Glue成员账户，列出名称Amazon Glue在账户中创建的工作流程，列表可用Amazon Glue账户的工作组；检索有关Amazon Amazon 的详细信息 GuardDuty 筛选器，检索GuardDuty IPset，检索一个GuardDuty ThreatIntelSet，检索检索 GuardDuty 成员账户，获取清单GuardDuty 过滤器，获取 GuardDuty服务，检索的标签 GuardDuty 服务，然后得到ThreatIntelSets 的 GuardDuty 服务；获取 Amazon Macie 账户的当前状态和配置设置；检索资源和委托人关联Amazon Resource Access Manager(Amazon RAM)资源共享并检索有关的详细信息Amazon RAM资源共享；要获取有关 Amazon Simple Email Service (Amazon SES) 现有配置集的信息，获取与 Amazon SES 配置集关联的事件目标列表，列出与 Amazon SES 账户关联的所有配置集；以及获取身份列表中心目录属性，获取Amazon IAM Identity Center (successor to Amazon Single Sign-On)权限集，获取附加到指定的 IAM 托管策略IAM Identity Center权限集，获取的权限集IAM Identity Center	2022 年 5 月 31 日

更改	说明	日期
	实例，并获取标签IAM Identity Center资源的费用。	

更改	说明	日期
AWS_ConfigRole (p. 244)—添加雅典娜：GetDataCatalog，athena：ListDataCatalogs，athena：ListTagsForResource，detectiveListGraphs，detectiveListTagsForResource，glinke：BatchGetDevEndpoints，glinke：GetDevEndpoint，glinke：GetDevEndpoints，glinke：GetSecurityConfiguration，glinke：GetSecurityConfigurations，glinke：GetTags 粘附:GetWorkGroup，glue：ListCrawlers，glue：ListDevEndpoints，glue：ListJobs，glue：ListMembers，glue：ListWorkflows，glue：ListWorkGroups，guarduty：GetFilter，警卫职责：getipset，警卫职责：GetThreatIntelSet，guarduty：GetMembers，guarduty：ListFilters，警卫职责：listipsets，警卫职责：ListTagsForResource，guarduty：ListThreatIntelSets，macie：GetMacieSession, ram：GetResourceShareAssociations, ram：GetResourceShares，请参阅：GetConfigurationSet，请参阅：GetConfigurationSetEventDestinations，请参阅：ListConfigurationSets，所以：DescribeInstanceAccessControlAttributeConfiguration，所以：DescribePermissionSet，所以：ListManagedPoliciesInPermissionSet，所以：ListPermissionSets，等等：ListTagsForResource	此策略现在授予权限以获取指定的 Amazon Athena 数据目录，在Amazon账户，并列出与 Athena 工作组或数据目录资源关联的标签；获取 Amazon Detective 行为图表列表和 Detective 行为图的列表标签；获取给定列表的资源元数据列表Amazon Glue开发终端节点名称，获取有关指定终端节点的详细信息Amazon Glue开发端点，获取所有Amazon Glue开发终端节点位于Amazon账户，检索指定的Amazon Glue安全配置，全部获取Amazon Glue安全配置，获取与安全配置关联的标签列表Amazon Glue资源，获取有关的信息Amazon Glue具有指定名称的工作组，检索所有Amazon Glue爬虫资源位于Amazon账户，获取所有人的名字Amazon Glue `DevEndpoint`资源在Amazon账户，列出所有账户Amazon Glue中的任务资源Amazon账户，获取有关的详细信息Amazon Glue成员账户，列出名称Amazon Glue在账户中创建的工作流程，列表可用Amazon Glue账户的工作组；检索有关Amazon Amazon 的详细信息 GuardDuty 筛选器，检索GuardDuty IPset，检索一个GuardDuty ThreatIntelSet，检索检索 GuardDuty 成员账户，获取清单 GuardDuty 过滤器，获取 GuardDuty 服务，检索的标签 GuardDuty 服务，然后得到ThreatIntelSets 的 GuardDuty 服务，；获取 Amazon Macie 账户的当前状态和配置设置；检索资源和委托人关联Amazon Resource Access Manager(Amazon RAM)资源共享并检索有关的详细信息Amazon RAM资源共享；要获取有关 Amazon Simple Email Service (Amazon SES) 现有配置集的信息，获取与 Amazon SES 配置集关联的事件目标列表，列出与 Amazon SES 账户关联的所有配置集；以及获取身份列表中心目录属性，获取Amazon IAM Identity Center (successor to Amazon Single Sign-On)权限集，获取附加到指定的 IAM 托管策略IAM Identity Center权限集，获取的权限集IAM Identity Center	2022 年 5 月 31 日

更改	说明	日期
	实例，并获取标签IAM Identity Center资源的费用。	
AWSConfigServiceRolePolicy (p. 23)—添加云形态：GetResource，cloudfation：ListResources，cloudtraillGetEventDataStore，dax：DescribeParameterGroups，dax：DescribeParameters，dax：DescribeSubnetGroups, DMS：DescribeReplicationTasks，以及组织：ListPolicies	此策略现在授予权限以获取有关所有或指定的Amazon CloudTrail事件数据存储 (EDS)，获取有关所有或指定的AmazonCloudFormation资源，获取DynamoDB 加速器 (DAX) 参数组或子网组的列表，获取有关Amazon Database Migration Service(Amazon DMS) 在当前区域中用于您的账户的在当前区域中用于您的账户的在当前区域中用于您的账户的在当前区域中用于您的账户的的Amazon Organizations指定类型的。	2022 年 4 月 7 日
AWS_ConfigRole (p. 244)—添加云形态：GetResource，cloudfation：ListResources，cloudtrailGetEventDataStore，dax：DescribeParameterGroups，dax：DescribeParameters，dax：DescribeSubnetGroups, DMS：DescribeReplicationTasks，以及组织：ListPolicies	此策略现在授予权限以获取有关所有或指定的Amazon CloudTrail事件数据存储 (EDS)，获取有关所有或指定的AmazonCloudFormation资源，获取DynamoDB 加速器 (DAX) 参数组或子网组的列表，获取有关Amazon Database Migration Service(Amazon DMS) 在当前区域中用于您的账户的在当前区域中用于您的账户的在当前区域中用于您的账户的在当前区域中用于您的账户的的Amazon Organizations指定类型的。	2022 年 4 月 7 日

更改	说明	日期
AWSConfigServiceRolePolicy (p. 231) 添加备份网关：ListTagsForResource，备份网关：ListVirtualMachines，批处理：DescribeComputeEnvironments，批处理：DescribeJobQueues，批处理：ListTagsForResource，dax：ListTags，dams:DescribeCertificates，dynamodb：DescribeGlobalTable，dynamodb：DescribeGlobalTableSettings，ec2:DescribeClientVpnAuthorizationRules，ec2:DescribeClientVpnEndpoints，ec2:DescribeDhcpOptions，ec2:DescribeFleets，ec2:DescribeNetworkAcls，ec2:DescribePlacementGroups，ec2:DescribeSpotFleetRequests，ec2:DescribeVolumeAttribute，ec2:DescribeVolumes，ek:DescribeFargateProfile，eks：ListFargateProfiles, eks：ListTagsForResource，fsx：ListTagsForResource，guarduty：ListOrganizationAdminAccounts，kms:ListAliases，opsworks：DescribeLayers，opsworks：DescribeStacks，opsworks：ListTags，rds:describedbClusterParameterGroups，rds:describedbClusterParameters，指出：DescribeActivity，指出：ListActivities，wafv2：GetRuleGroup，wafv2：ListRuleGroups，wafv2：ListTagsForResource，workspaces：DescribeConnectionAliases，workspaces：DescribeTags和WS; 和WS; WS;DescribeWorkspaces	此策略现在支持的额外权限 Amazon Backup、Amazon Batch、DynamoDB AccccAmazon Database Migration Service、Amazon DynamoDB、亚马逊Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Kubernetes Service、Amazon FSx GuardDuty、Amazon Key Management Service、Amazon OpsWorks、Amazon Relational Database Service ationAmazon WAFV2 和亚马逊 WorkSpaces.	2022 年 3 月 14 日

更改	说明	日期
AWS_ConfigRole (p. 244)—添加备份网关：ListTagsForResource，备份网关：ListVirtualMachines，批处理：DescribeComputeEnvironments，批处理：DescribeJobQueues，批处理：ListTagsForResource，dax：ListTags, dms：DescribeCertificates，dynamodb：DescribeGlobalTable，dynamodb：DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks：DescribeFargateProfile, eks：ListFargateProfiles, eks：ListTagsForResource，fsx：ListTagsForResource，guarduty：ListOrganizationAdminAccounts, kms:ListAliases，opsworks：DescribeLayers，opsworks：DescribeStacks，opsworks：ListTags，rds: describedbClusterParameterGroups，rds: describedbClusterParameters，指出：DescribeActivity，指出：ListActivities，wafv2：GetRuleGroup，wafv2：ListRuleGroups，wafv2：ListTagsForResource，workspaces：DescribeConnectionAliases，workspaces：DescribeTags和WS; 和WS; WS;DescribeWorkspaces	此策略现在支持的额外权限 Amazon Backup、Amazon Batch、DynamoDB AccccAmazon Database Migration Service、Amazon DynamoDB、亚马逊Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Kubernetes Service、Amazon FSx GuardDuty、Amazon Key Management Service、Amazon OpsWorks、Amazon Relational Database Service ationAmazon WAFV2 和亚马逊 WorkSpaces.	2022 年 3 月 14 日

更改	说明	日期
AWSConfigServiceRolePolicy (p. 23)— 添加弹性豆茎：DescribeEnvironments，弹性豆茎：DescribeConfigurationSettings，账户：GetAlternateContact，OrganizDescribePolicy，OrganizListPoliciesForTarget，eses:GetCompatibleElasticsearchVersions，rs：DescribeOptionGroups，rs：DescribeOptionGroups，eses:GetCompatibleVersions，codeartifact：GetRepositoryPolicy，access-access-GetArchiveRule，以及ecs：ListTaskDefinitionFamilies	此策略现在授予权限以获取有关 Elastic Beanstalk 环境的详细信息以及指定 Elastic Beanstalk 配置集的设置描述、获取 OpenSearch 或 Elasticsearch 版本，描述数据库的可用的 Amazon RDS 选项组，并获取有关 CodeDeploy 部署配置，此策略现在还授予权限以检索附加到的指定备用联系人 Amazon账户，检索有关的信息 Amazon CloudFormation 策略，检索 Amazon ECR 存储库策略，检索有关已存档的Amazon Config规则，检索 Amazon ECS 任务定义系列的列表，列出指定子 OU 或账户的根或父组织单位 (OU)，并列出附加到指定目标根、组织单位或账户的策略。	2022 年 2 月 10 日
AWS_ConfigRole (p. 244)— 添加弹性豆茎：DescribeEnvironments，弹性豆茎：DescribeConfigurationSettings，账户：GetAlternateContact，OrganizDescribePolicy，OrganizListPoliciesForTarget，eses:GetCompatibleElasticsearchVersions，rs：DescribeOptionGroups，rs：DescribeOptionGroups，eses:GetCompatibleVersions，codeartifact：GetRepositoryPolicy，access-access-GetArchiveRule，以及ecs：ListTaskDefinitionFamilies	此策略现在授予权限以获取有关 Elastic Beanstalk 环境的详细信息以及指定 Elastic Beanstalk 配置集的设置描述、获取 OpenSearch 或 Elasticsearch 版本，描述数据库的可用的 Amazon RDS 选项组，并获取有关 CodeDeploy 部署配置，此策略现在还授予权限以检索附加到的指定备用联系人 Amazon账户，检索有关的信息 Amazon CloudFormation 策略，检索 Amazon ECR 存储库策略，检索有关已存档的Amazon Config规则，检索 Amazon ECS 任务定义系列的列表，列出指定子 OU 或账户的根或父组织单位 (OU)，并列出附加到指定目标根、组织单位或账户的策略。	2022 年 2 月 10 日
AWSConfigServiceRolePolicy (p. 23)— 添加日志：CreateLogStream，日志：CreateLogGroup，以及日志：PutLogEvent	此策略现在授予创建亚马逊的权限 CloudWatch 日志组和流，并将日志写入已创建的日志流。	2021 年 12 月 15 日
AWS_ConfigRole (p. 244)— 添加日志：CreateLogStream，日志：CreateLogGroup，以及日志：PutLogEvent	此策略现在授予创建亚马逊的权限 CloudWatch 日志组和流，并将日志写入已创建的日志流。	2021 年 12 月 15 日

更改	说明	日期
AWSConfigServiceRolePolicy (p. 23) AVE：DescribeDomain, eses:DescribeDomains、rds: describedbeDbParameters 和 elasticache:DescribeSnapshots	此策略现在授予获取有关Amazon Amazon Amazon 的详细信息权限 OpenSearch 服务 (OpenSearch 服务）域/域，并获取特定 Amazon 关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表。此政策还授予获取亚马逊详情的权限 ElastiCache 快照。	2021 年 9 月 8 日
AWS_ConfigRole (p. 244)— AVE：DescribeDomain, eses:DescribeDomains、rds: describedbeDbParameters 和 elasticache:DescribeSnapshots	此策略现在授予获取有关Amazon Amazon Amazon 的详细信息权限 OpenSearch 服务 (OpenSearch 服务）域/域，并获取特定 Amazon 关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表。此政策还授予获取亚马逊详情的权限 ElastiCache 快照。	2021 年 9 月 8 日
AWSConfigServiceRolePolicy (p. 23) 添加日志：ListTagsLogGroup，指出：ListTagsForResource，指出：ListStateMachines，指出：DescribeStateMachine，以及针对的额外权限Amazon资源类型	此策略现在授予列出日志组的标签、列出状态机的标签以及列出所有状态机的权限。此策略现在授予权限以获取有关状态机的详细信息。此策略现在还支持 Amazon EC2 系统管理器 (SSM)、亚马逊弹性容器注册表、亚马逊 FSX、Amazon Kinesis Data Firehose、Amazon Kinesis Data Firehose、Amazon MSK、Amazon Relational Database Service (Amazon RDS)、亚马逊 Route 53、亚马逊的其他权限 SageMaker、Amazon Simple SimpleAmazon Database Migration Service、Amazon Global Accelerator, 和Amazon Storage Gateway.	2021 年 7 月 28 日

更改	说明	日期
AWS_ConfigRole (p. 244)— 添加日志：ListTagsLogGroup，指出：ListTagsForResource，指出：ListStateMachines，指出：DescribeStateMachine，以及针对的额外权限Amazon资源类型	此策略现在授予列出日志组的标签、列出状态机的标签以及列出所有状态机的权限。此策略现在授予权限以获取有关状态机的详细信息。此策略现在还支持 Amazon EC2 系统管理器 (SSM)、亚马逊弹性容器注册表、亚马逊 FSX、Amazon Kinesis Data Firehose、Amazon Kinesis Data Firehose、Amazon MSK、Amazon Relational Database Service (Amazon RDS)、亚马逊 Route 53、亚马逊的其他权限 SageMaker、Amazon Simple SimpleAmazon Database Migration Service、Amazon Global Accelerator, 和Amazon Storage Gateway.	2021 年 7 月 28 日
AWSConfigServiceRolePolicy (p. 23添加短信号：DescribeDocumentPermission 以及额外权限Amazon资源类型	此策略现在授予权限Amazon Systems Manager有关 IAM 访问分析器的文档和信息。此策略现在支持其他AmazonAmazon Kinesis 的资源类型、亚马逊 ElastiCache、Amazon EMR、Amazon Network Firewall、AmaAmazon Relational Database Service on Route 53 这些权限更改允许Amazon Config调用支持这些资源类型所需的只读 API。此策略现在还支持过滤 Lambda @Edge 函数lambda-inside-vpc Amazon Config管理的规则。	2021 年 6 月 8 日
AWS_ConfigRole (p. 244)— 添加短信号：DescribeDocumentPermission 以及额外权限Amazon资源类型	此策略现在授予权限Amazon Systems Manager有关 IAM 访问分析器的文档和信息。此策略现在支持其他AmazonAmazon Kinesis 的资源类型、亚马逊 ElastiCache、Amazon EMR、Amazon Network Firewall、Amazon Route 53 和 Amazon Relational Database Service (Amazon RDS)。这些权限更改允许Amazon Config调用支持这些资源类型所需的只读 API。此策略现在还支持过滤 Lambda @Edge 函数lambda-inside-vpc Amazon Config管理的规则。	2021 年 6 月 8 日

更改	说明	日期
AWSConfigServiceRolePolicy (p. 231)— 添加 apiGateway: Get 对 API Gateway 和 s3 进行只读 GET 调用的权限：GetAccessPointPolicy 权限和 s3:GetAccessPointPolicyStatus 权限以调用 Amazon S3 只读 API	此策略现在授予的权限允许 Amazon Config对 API Gateway 进行只读 GET 调用以支持 Amazon ConfigAPI Geway (API Gateway 该策略还添加了允许Amazon Config调用Amazon Simple Storage Service (Amazon S3) 只读 API，这些应用程序是支持新的`AWS::S3::AccessPoint`资源类型。	2021 年 5 月 10 日
AWS_ConfigRole (p. 244)— 添加 apiGateway: Get 对 API Gateway 和 s3 进行只读 GET 调用的权限：GetAccessPointPolicy 权限和 s3:GetAccessPointPolicyStatus 权限以调用 Amazon S3 只读 API	此策略现在授予的权限允许 Amazon Config对 API Gateway 进行只读 GET 调用以支持 Amazon Config为 API Gateway。该策略还添加了允许Amazon Config调用Amazon Simple Storage Service (Amazon S3) 只读 API，这些应用程序是支持新的`AWS::S3::AccessPoint`资源类型。	2021 年 5 月 10 日
AWSConfigServiceRolePolicy (p. 231)— 添加 sm：ListDocuments 权限和其他权限Amazon资源类型	此策略现在授予权限Amazon Systems Manager指定的文档。此策略现在还支持其他Amazon的资源类型Amazon Backup、Amazon Elastic File System ic ElastiCache、Amazon Simple Storage Service (Amazon S3)、Amazon Kinesis、Amazon Kinesis、Amaz SageMaker、Amazon Database Migration Service，以及Amazon Route 53。这些权限更改允许Amazon Config调用支持这些资源类型所需的只读 API。	2021 年 4 月 1 日
AWS_ConfigRole (p. 244)— 添加 sm：ListDocuments 权限和其他权限Amazon资源类型	此策略现在授予权限Amazon Systems Manager指定的文档。此策略现在还支持其他Amazon的资源类型Amazon Backup、Amazon Elastic File System ic ElastiCache、Amazon Simple Storage Service (Amazon S3)、Amazon Kinesis、Amazon Kinesis、Amaz SageMaker、Amazon Database Migration Service，以及Amazon Route 53。这些权限更改允许Amazon Config调用支持这些资源类型所需的只读 API。	2021 年 4 月 1 日
`AWSConfigRole`已淘汰	`AWSConfigRole`已淘汰。换货政策是`AWS_ConfigRole`.	2021 年 4 月 1 日

更改	说明	日期
Amazon Config 已开启跟踪更改	Amazon Config 为其 Amazon 托管式策略开启了跟踪更改。	2021 年 4 月 1 日

Amazon Config 中的日志记录和监控

Amazon Config 与 Amazon CloudTrail 集成，后者是在 Amazon 中记录用户、角色或 Amazon Config 服务所执行操作的服务。监控是保持 Amazon Config 和您的 Amazon 解决方案的可靠性、可用性和性能的重要方面。

使用 Amazon CloudTrail 记录 Amazon Config API 调用

CloudTrail 会捕获的所有 API 调用Amazon Config作为事件。捕获的调用包含来自 Amazon Config 控制台和代码的 Amazon Config API 操作调用。如果您创建了跟踪，则可以启用 CloudTrail 事件记录到 Amazon S3 存储桶，包括针对的事件Amazon Config. 如果您不配置跟踪，则仍可在 CloudTrail 控制台在事件历史记录. 使用收集的信息 CloudTrail，则可以确定已对发出的请求Amazon Config、发出请求的源 IP 地址、用户、请求时间以及其他详细信息。

了解相关更多信息 CloudTrail，请参阅Amazon CloudTrail用户指南.

主题

- Amazon Config中的 信息 CloudTrail (p. 267)
- 了解 Amazon Config 日志文件条目 (p. 268)
- 示例日志文件 (p. 268)

Amazon Config中的 信息 CloudTrail

CloudTrail 已在您的 FS 上启用Amazon在您创建账户时。当活动发生在Amazon Config，该活动记录在 CloudTrail 事件以及其他Amazon中的服务事件事件历史记录. 您可以在 Amazon 账户中查看、搜索和下载最新事件。有关更多信息，请参阅 。使用查看事件 CloudTrail 事件历史记录.

要持续记录 Amazon 账户中的事件（包括 Amazon Config 的事件），请创建跟踪。一个踪迹启用 CloudTrail ，用于将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有Amazon Web Services 区域。此跟踪记录在 Amazon 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）存储桶。此外，您还可以配置其他Amazon服务 CloudTrail 日志。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
- 为 配置 Amazon SNS 通知 CloudTrail
- 接收 CloudTrail 多个区域中的日志文件和接收 CloudTrail 多个账户中的日志文件

全部Amazon Config操作由记录 CloudTrail 并记录在Amazon ConfigAPI 参考. 例如，对DeliverConfigSnapshot、DeleteDeliveryChannel, 和DescribeDeliveryChannels操作在 CloudTrail 日志文件。

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

- 请求是使用根用户凭证还是 Amazon Identity and Access Management (IAM) 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。

- 请求是否由其它 Amazon 服务发出。

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

了解 Amazon Config 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。 CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

示例日志文件

举个例子 CloudTrail 日志条目，请参阅以下主题。

目录

DeleteDeliveryChannel

以下示例： CloudTrail 日志文件DeleteDeliveryChanneloperation.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DeliverConfigSnapshot

以下示例： CloudTrail 日志文件DeliverConfigSnapshotoperation.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```


DescribeConfigurationRecorderStatus

以下示例： CloudTrail 日志文件DescribeConfigurationRecorderStatusoperation.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
```

```
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```


DescribeConfigurationRecorders

以下示例： CloudTrail 日志文件DescribeConfigurationRecordersoperation.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```


DescribeDeliveryChannels

以下是一个示例 CloudTrail 日志文件DescribeDeliveryChannelsoperation.


```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
```

```
    }
```

GetResourceConfigHistory

以下示例： CloudTrail 日志文件GetResourceConfigHistoryoperation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

以下示例： CloudTrail 日志文件PutConfigurationRecorderoperation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:23Z",
```

```
      "eventSource": "config.amazonaws.com",
      "eventName": "PutConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorder": {
          "name": "default",
          "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
        }
      },
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

以下示例： CloudTrail 日志文件PutDeliveryChanneloperation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

以下示例： CloudTrail 日志文件StartConfigurationRecorderoperation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
```

```
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

以下示例： CloudTrail 日志文件StopConfigurationRecorderoperation.

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

监控

你可以用其他Amazon监控的服务Amazon Config资源的费用。

- 每当支持时，您可以使用 Amazon Simple Notification Service (SNS) 向您发送通知Amazon资源是用户通过 API 对资源进行创建、更新或修改的。
- 你可以使用亚马逊 CloudWatch 检测状态变更并对其进行响应的事件Amazon Config事件.

主题

监控AmazonAmazon SQS 的资源变更

Amazon Config每当支持的 Amazon Simple Notification Service (SNS) 向您发送通知Amazon资源是用户通过 API 对资源进行创建、更新或修改的。但是您可能只关注特定资源配置的更改。例如，您可能认为必须在有人修改了安全组配置时了解这一情况，但不需要在您的Amazon EC2 实例上的标签每次更改时都得到通知。或者，您可能想要编写一个在指定资源被更新时执行指定操作的程序。例如，您可能想要在某个安全组的配置发生更改时启动特定工作流程。如果要以编程方式使用来自的数据Amazon Config以上述目的或其他方式，使用 Amazon Simple Queue Service 队列作为 Amazon SNS 的通知终端节点。

> Note
>
> Amazon SNS 发出的通知的形式可以是电子邮件、发送到支持短信服务功能的手机和智能手机上的短信服务 (SMS) 消息、发送到移动设备应用程序上的通知消息，或者发送到一个或多个 HTTP 或 HTTPS 终端节点的通知消息。

无论每个区域只订阅一个主题还是每个区域的每个账户只订阅一个主题，您都可以使用单个 SQS 队列订阅多个主题。您必须用队列订阅您需要的 SNS 主题。(您可以用多个队列订阅一个 SNS 主题。) 有关更多信息，请参阅 。将 Amazon SNS 消息发送至 Amazon SQS 队列.

Amazon SQS 的权限

要将 Amazon SQS 与Amazon Config、您必须配置一项策略，该策略将向您的账户授予权限，以便对 SQS 队列执行允许的所有操作。以下示例策略授予账户 111122223333 和 444455556666 权限，允许其在名为 arn:aws:sqs:us-east-2:444455556666:queue1. 的队列每次发生配置更改时发送相关消息。

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

您还必须创建一项策略，授予 SNS 主题和订阅该主题的 SQS 队列之间的连接权限。以下是一个示例策略，该策略允许具有Amazon 资源名称 (ARN) 的 SNS 主题 arn: aws: sns: us-east-2:111122223333: test-topic 对名为 arn: aws: sqs: us-east-2:111122223333 的队列执行任何操作：test-topic-queue.

> Note
>
> SNS 主题和 SQS 队列的账户必须处于同一区域中。

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
```

```
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

每项策略中的规定可以只针对一个队列而不是多个队列。有关 Amazon SQS 策略受到的其他限制的信息，请参阅Amazon SQS 策略的特殊信息.

监控Amazon Config和 Amazon EventBridge

亚马逊 EventBridge 提供近乎实时的系统事件流，这些系统事件描述在Amazon资源的费用。使用 Amazon EventBridge 检测状态的变更并对其进行响应Amazon Config事件.

您可以创建一个规则，只要状态发生变换或者在变换到一个或多个感兴趣的状态时，就运行该规则。然后，根据您创建的规则，亚马逊 EventBridge 在事件匹配您在规则中指定的值时调用一个或多个目标操作。根据事件类型，您可能想要发送通知、捕获事件信息、采取纠正措施、启动事件或采取其他操作。

然而，在为 Amazon Config 创建事件规则之前，您应当执行以下操作：

- 熟悉中的事件、规则和目标 EventBridge. 有关更多信息，请参阅 。什么是 Amazon EventBridge?
- 有关如何开始使用的更多信息 EventBridge 并设置规则，请参阅。Amazon 入门 EventBridge.
- 创建将在您的事件规则中使用的目标。

主题

亚马逊 EventBridge 适用于 的 格式Amazon Config

这些区域有： EventBridge 事件为了Amazon Config格式如下：

```
        {
           "version": "0",
           "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
           "detail-type": "event type",
           "source": "aws.config",
           "account": "111122223333",
           "time": "2018-03-22T00:38:11Z",
           "region": "us-east-1",
           "resources": [
              resources
           ],
           "detail": {
              specific message type
           }
        }
```

创建Amazon EventBridge 规则Amazon Config

按照以下步骤创建一个 EventBridge 对由发出的事件触发的规则Amazon Config. 尽最大努力发出事件。

1. 在导航窗格中，选择 Rules (规则)。
2. 选择 Create rule (创建规则)。
3. 为规则输入名称和描述。

   规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。
4. 对于 Define pattern (定义模式)，选择 Event pattern (事件模式)。
5. 选择服务预定义的模式
6. 对于 Service provider（服务提供商），选择 Amazon。
7. 适用于Service name (服务名称)，选择Config.
8. 对于 Event Type，选择用于触发此规则的事件类型：
   - 选择所有事件以制定一个应用于所有人的规则Amazon服务。如果您选择此选项，则不能选择特定的消息类型、规则名称、资源类型或资源 ID。
   - 选择AmazonAPI 调用的 API CloudTrail以使规则基于对此服务进行的 API 调用。有关创建此类规则的更多信息，请参阅教程：创建 Amazon 创 EventBridge 规则Amazon CloudTrailAPI 调用.
   - 选择 Config Configuration Item Change 以在您账户中的资源发生更改时获取通知。

     如这些支持文章中所述，你可以使用 EventBridge 要在创建或删除资源时接收自定义电子邮件通知，在我的中创建资源时，如何接收自定义电子邮件通知Amazon账户使用Amazon Config服务？和当我的资源被删除时，我怎样才能收到自定义电子邮件通知Amazon账户使用Amazon Config服务？.
   - 选择 Config Rules Compliance Change 以在对您的规则进行合规性检查失败时获取通知。

     如本支持文章中所述，您可以使用 EventBridge 要在资源不合规时接收自定义电子邮件通知，如何确定何时收到通知Amazon资源使用不合规Amazon Config?.
   - 选择 Config Rules Re-evaluation Status 以获取重新评估状态通知。
   - 选择 Config Configuration Snapshot Delivery Status 以获取配置快照传输状态通知。
   - 选择 Config Configuration History Delivery Status 以获取配置历史记录传输状态通知。
9. 选择 Any message type 以接收任何类型的通知。选择 Specific message type(s) 以接收以下类型的通知：
   - 如果选择...ConfigurationItemChangeNotification，当你收到消息时Amazon Config已成功将配置快照传送到 Amazon S3 存储桶。
   - 如果选择...ComplianceChangeNotification，则会在资源的合规性类型符合以下条件时收到消息Amazon Config评估已更改。
   - 如果选择...ConfigRulesEvaluationStarted，当你收到消息时Amazon Config开始针对指定的资源评估您的规则。
   - 如果选择...ConfigurationSnapshotDeliveryCompleted，当你收到消息时Amazon Config已成功将配置快照传送到 Amazon S3 存储桶。
   - 如果选择...ConfigurationSnapshotDeliveryFailed，当你收到消息时Amazon Config未能将配置快照传送到 Amazon S3 存储桶。
   - 如果选择...ConfigurationSnapshotDeliveryStarted，当你收到消息时Amazon Config开始向您的 Amazon S3 存储桶传送配置快照。
   - 如果选择...ConfigurationHistoryDeliveryCompleted，当你收到消息时Amazon Config已成功将配置历史记录传送到 Amazon S3 存储桶。
10. 如果您从中选择了特定的事件类型事件类型下拉列表中，选择任意资源类型以制定一个应用于所有人的规则Amazon Config支持的资源类型：

    或者，选择 Specific resource type(s) (特定资源类型)，然后键入 Amazon Config 支持的资源类型（例如，`AWS::EC2::Instance`）。
11. 如果您从中选择了特定的事件类型事件类型下拉列表中，选择任意资源 ID包括任何Amazon Config支持的资源 ID。

    或者，选择 Specific resource ID(s) (特定资源 ID)，然后键入 Amazon Config 支持的资源 ID（例如，`i-04606de676e635647`）。

12.如果您从中选择了特定的事件类型事件类型下拉列表中，选择任何规则名称包括任何Amazon Config支持的规则。

或者，选择 Specific rule name(s) (特定规则名称)，然后键入 Amazon Config 支持的规则（例如，required-tags）。

13.对于 Select event bus（选择事件总线），请选择要与此规则关联的事件总线。如果您希望此规则对来自您自己的账户的匹配事件触发，请选择 Amazon 原定设置事件总线。当您账户中的某个 Amazon 服务发出一个事件时，它始终会发送到您账户的默认事件总线。

14.适用于选择目标，选择您准备为此规则使用的目标类型，然后配置该类型所需的任何其他选项。

15.根据您选择的服务，显示的字段会有所不同。根据需要输入特定于此目标类型的信息。

16.对于许多目标类型， EventBridge 需要权限以便将事件发送到目标。在这些情况下， EventBridge 可以创建运行任务所需的 IAM 角色。

- 若要自动创建 IAM 角色，请选择 Create a new role for this specific resource (为此特定资源创建新角色)。
- 要使用您之前创建的 IAM 角色，请选择 Use existing role (使用现有角色)。

17.对于重试策略和死信队列：，在重试策略下：

- 对于 Maximum age of event（事件的最大时长），输入一分钟（00:01）与 24 小时（24:00）之间的值。
- 对于重试尝试，输入 0 到 185 之间的数字。

18.适用于死信队列列列中，选择是否使用标准 Amazon SQS 队列作为死信队列。 EventBridge 如果与此规则匹配的事件未成功传递到目标，会将这些事件发送到死信队列。请执行下列操作之一：

- 选择无不使用死信队列。
- 选择选择当前的 Amazon SQS 队列Amazon用作死信队列的账户，然后从下拉列表中选择要使用的队列。
- 选择在其他 Amazon SQS 队列中选择其他队列 Amazon 帐户作为死信队列，然后输入要使用的队列的 ARN。您必须将基于资源的策略附加到队列 EventBridge 向其发送消息的权限。有关更多信息，请参阅 。事件重试策略和使用死信队列.

19.（可选）选择 Add target (添加目标)，以便为此规则添加另一个目标。

20.（可选）为规则输入一个或多个标签。有关更多信息，请参阅 。亚马逊 EventBridge 标签.

21.审查您的规则设置以确保其符合事件监控要求。

22.选择Create以确认您的选择。

使用Amazon Config使用 Amazon VPC 终端节

如果您使用 Amazon Virtual Private Cloud（Amazon VPC）托管 Amazon 资源，则可以在您的 VPC 和 Amazon Config 之间建立私有连接。您可以使用此连接从您的 VPC 上与 Amazon Config 通信而不用访问公共 Internet。

Amazon VPC 是一项 Amazon 服务，可用来启动在虚拟网络中定义的 Amazon 资源。借助 VPC，您可以控制您的网络设置，如 IP 地址范围、子网、路由表和网络网关。接口 VPC 终端节点由Amazon PrivateLink，一个Amazon实现私人通信的技术Amazon使用具有私有 IP 地址的elastic network interface 的服务。要将 VPC 连接到 Amazon Config，请为 Amazon Config 定义一个接口 VPC 终端节点。这种类型的端点使您能够将 VPC 连接到Amazon服务。该终端节点提供了到 Amazon Config 的可靠、可扩展的连接，无需 Internet 网关、网络地址转换 (NAT) 实例或 VPN 连接。有关更多信息，请参阅 Amazon VPC 用户指南中的什么是 Amazon VPC。

以下步骤适用于 Amazon VPC 的用户。有关更多信息，请参阅 Amazon VPC 用户指南中的开始使用。

可用性

Amazon Config 当前在以下区域中支持 VPC 终端节点：

- 美国东部（俄亥俄）
- 美国东部（弗吉尼亚北部）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈）
- Asia Pacific (Mumbai)
- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太区域（东京）
- 加拿大（中部）
- 欧洲（法兰克福）
- 欧洲（爱尔兰）
- 欧洲（伦敦）
- 欧洲（巴黎）
- 南美洲（圣保罗）
- 亚太地区（香港）
- 非洲（开普敦）
- 欧洲（米兰）
- Europe (Stockholm)
- 中东（巴林）
- Amazon GovCloud (US-t)
- Amazon GovCloud (US-西部)

为 Amazon Config 创建 VPC 终端节点

要开始将您的 Amazon Config 与 VPC 一起使用，请为 Amazon Config 创建接口 VPC 终端节点。您无需更改 Amazon Config 的设置。Amazon Config 将调用使用自身的公有终端节点的其他 Amazon 服务。有关更多信息，请参阅 Amazon VPC 用户指南中的创建接口端点。

Amazon Config 中的事件响应

Amazon Config 的事件响应是一项 Amazon 责任。Amazon 拥有正式的、已归档的策略和程序来管理事件响应。

具有广泛影响的 Amazon 操作性问题将在 Amazon 服务运行状况控制面板上发布。操作性问题也会通过 Personal Health Dashboard 发布给个人账户。

Amazon Config 的合规性验证

作为多个 Amazon Config 合规性计划的一部分，第三方审核员将评估 Amazon 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

要了解此服务或其他 Amazon Web Services 是否在特定合规性计划范围内，请参阅合规性计划范围内的 Amazon Web Services。有关常规信息，请参阅Amazon Web Services合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅、在 Amazon Artifact 中下载报告。

您使用 Amazon Web Services 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。Amazon 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在Amazon上部署注重安全性和合规性的基准环境的步骤。
- 亚马逊云科技上的 HIPAA 安全性和合规性架构设计 – 此白皮书介绍了企业如何使用 Amazon Web Services 创建符合 HIPAA 要求的应用程序。

  Note

  并非所有 Amazon Web Services都符合 HIPAA 要求。有关更多信息，请参阅符合 HIPAA 要求的服务参考。
- Amazon合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config 开发人员指南中的使用规则评估资源 – 此 Amazon Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub：此 Amazon Web Service 提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践规范。

Amazon Config 中的故障恢复能力

Amazon全球基础设施围绕Amazon区域和可用区构建。Amazon区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 Amazon 区域和可用区的更多信息，请参阅 Amazon 全球基础设施。

Amazon Config 中的基础设施安全性

作为一项托管服务，Amazon Config受保护Amazon全局网络安全过程在Amazon Web Services：安全过程概述白皮书。

您可以使用 Amazon 发布的 API 调用通过网络访问 Amazon Config。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service (Amazon STS) 生成临时安全凭证来对请求进行签名。

配置和漏洞分析

对于 Amazon Config，Amazon 负责处理来宾操作系统 (OS) 和数据库补丁、防火墙配置和灾难恢复等基本安全任务。

Amazon Config 的安全最佳实践

Amazon Config 提供了在您开发和实施自己的安全策略时需要考虑的大量安全功能。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合您的环境或不满足您的环境要求，请将其视为有用的考虑因素而不是惯例。

- 利用 Amazon Config 的标记，这样便于管理、搜索和筛选资源。
- 确认您的传输通道已正确设置，确认后，验证 Amazon Config 是否正确记录。

有关更多信息，请参阅 。Amazon Config最佳实践博客。

Amazon Config 资源

下列相关资源在您使用此服务的过程中会有所帮助。

- Amazon Config – 提供 Amazon Config 相关信息的主要网页。
- Amazon Config 定价
- 技术方面常见问题
- Amazon Config规则开发工具包 (RDK)— 一种可以帮助您设置的开源工具Amazon Config，作者规则，然后使用各种Amazon资源类型。
- 合作伙伴— 链接到与之完全集成的合作伙伴产品Amazon Config可以帮助您直观呈现、监控并管理来自您的配置流、配置快照或配置历史记录的数据。

- 课程和研讨会 – 指向基于角色的专业课程和自主进度动手实验室的链接，这些课程和实验室旨在帮助您增强 Amazon 技能并获得实践经验。
- Amazon开发人员工具 – 指向开发人员工具、开发工具包、IDE 工具包和命令行工具的链接，这些资源用于开发和管理Amazon应用程序。
- Amazon白皮书 – 指向Amazon技术白皮书的完整列表的链接，这些资料涵盖了架构、安全性、经济性等主题，由Amazon解决方案架构师或其他技术专家编写。
- Amazon Web Services Support 中心 – 用于创建和管理 Amazon Web Services Support 案例的中心。还提供指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况以及Amazon Trusted Advisor。
- Amazon Web Services Support— 提供有关信息的主要网页Amazon Web Services Support，aone-on-one，快速响应支持渠道，可帮助您在云中构建和运行应用程序。
- 联系我们 – 用于查询有关Amazon账单、账户、事件、滥用和其他问题的中央联系点。
- Amazon网站条款 – 有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

适用于 Amazon Config 的 Amazon 软件开发工具包

Amazon 软件开发工具包使用户可以更轻松地构建应用程序，以对经济高效、可扩展而又可靠的 Amazon 基础设施服务进行访问。Amazon 软件开发工具包是可下载的单个软件包，其中包含库、代码示例和参考文档，您可以在几分钟内开始使用。下表列出了可用的软件开发工具包和第三方库，以便您以编程方式访问 Amazon Config。

访问类型	说明
Amazon 开发工具包	Amazon 提供以下软件开发工具包： • 适用于 C++ 文档的 Amazon 开发工具包 • Amazon Mobile SDK for iOS 文档 • 适用于 Go 文档的 Amazon 开发工具包 • Amazon SDK for Java 文档 • Amazon适用于JavaScript文档 • Amazon SDK for .NET 文档 • Amazon SDK for PHP 文档 • Amazon SDK for Python (Boto) 文档 • Amazon SDK for Ruby 文档

访问类型	说明
第三方库	Amazon 开发人员社区中的开发人员还会提供他们自己的库，您可以在以下 Amazon 开发人员中心获取这些资源： • Amazon Java 开发人员中心 • Amazon JavaScript开发人员中心 • AmazonPHP 开发人员中心 • Amazon Python 开发者中心 • Amazon Ruby 开发人员中心 • Amazon Windows 和 .NET 开发人员中心

常见问题

对的更改Amazon Config资源关系

主题

新的变化是什么Amazon Config资源关系？

为了优化记录的资源变化数量，Amazon Config将发布在配置项目 (CI) 中为七种 Amazon EC2 资源类型建模的关系的更新。此更新针对 Amazon EC2 实例、安全组、网络接口、子网、VPC、VPN 网关和客户网关资源类型优化了 CI 模型，以记录直接关系并弃用间接关系。

与资源相关的直接和直接关系是什么？

直接关系定义为资源 (A) 和另一资源 (B) 之间的单向关系 (A->B)，通常来自资源 (A) 的描述 API 响应。另一方面，间接关系是一种关系Amazon Config推导者（B->A），以便建立双向关系。例如，Amazon EC2 实例-> 安全组是直接关系，因为安全组将作为 Amazon EC2 实例的描述 API 响应的一部分返回。但是安全组-> Amazon EC2实例是间接关系，因为在描述 Amazon EC2 安全组时，不会返回 Amazon EC2 实例。

这种变化的好处是什么？Amazon Config订阅者？

通过弃用间接关系，与关系更改相关的配置项目减少了。这可能有助于遏制Amazon Config成本尤其是在临时工作负载的情况下，Amazon EC2 资源类型的配置更改大量。

哪些资源关系正在被删除？

以下资源关系将被弃用。

资源类型	与资源类型的间接关系		
AWS::EC2::CustomerGateway	AWS::EC2::VPNConnection		
AWS::EC2::Instance	AWS::EC2::EIP, AWS::EC2::RouteTable		
AWS::EC2::NetworkInterface	AWS::EC2::EIP, AWS::EC2::RouteTable		

资源类型	与资源类型的间接关系		
AWS::EC2::SecurityGroup	AWS::EC2::Instance, AWS::EC2::NetworkInterface		
AWS::EC2::Subnet	AWS::EC2::Instance, AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable		
AWS::EC2::VPNGateway	AWS::EC2::RouteTable, AWS::EC2::VPNConnection		

如何Amazon Config托管规则受影响？

Amazon Config在上面列出的资源之一上触发的托管规则将由Amazon Config团队。如果您尚未为这些规则定义标签，则不需要采取任何行动。如果定义了标签，则可能需要更新托管规则的标签。

具体来说，Amazon Config托管规则ec2security-group-attached-to-eni (p. 147)受到影响，因为一旦间接关系被弃用，触发此规则的配置项将不再创建。如果您使用此规则，请将其从评估的配置中删除Amazon资源并将其替换为新的ec2-security-group-attached-to-eni-期期性规则。这些区域有：ec2-security-group-attached-to-eni-期期性规则不会受到此弃用的影响，因为它是定期触发的，而不是配置更改。

对自定义的确切影响是什么Amazon Config对这些资源类型使用配置触发器的规则？

如果您使用的自定义规则不是由上表中列出的资源触发的，则不需要采取进一步的操作。如果您有触发上表中的某个资源的规则，请检查该规则以确定“合规”状态是否需要来自表中列出关系的另一个资源的信息。资源关系的更改将导致触发的更改减少，因为间接关系（如上表所列）将不再被跟踪。如果信息对规则的实施逻辑至关重要，请添加相关资源作为附加配置触发器，或者使用高级查询。

我是否应该预计会延迟报告带有配置更改的托管规则的评估结果？

任何受此更改影响的托管规则都将被更新。在报告具有配置更改的托管规则的评估结果时，您不应该遇到任何延迟。

对历史数据的影响是什么？ 它还会显示有关间接关系的详细信息吗？

间接关系将在历史上可用`ConfigurationItems`在它们被弃用之前记录，但不会在`ConfigurationItems`弃用后记录。

产生的输出是否有变化`GetResourceConfigHistory`API？

中使用的模型`GetResourceConfigHistory`API 没有更改，返回的数据也没有更改`ConfigurationItems`在弃用之前记录。`ConfigurationItems`弃用后记录的不再包括关系字段中返回的子位置类型。

配置项目的资源架构有什么变化吗？

中的数据模式没有变化配置“配置项目” 中的字段。唯一的变化是关系“配置项” 中的字段将不再包括指定的间接关系。

还有其他替代方法可以检索间接关系吗？

启动高级查询后，您可以运行结构化查询语言 (SQL) 查询。例如，如果要检索与安全组相关的 EC2 实例列表，请使用以下查询：

```
SELECT
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

这里提供了示例关系查询：示例查询

以下代码示例Amazon Config使用Amazon软件开发工具包

以下代码示例显示了如何使用：Amazon Config用Amazon软件开发套件 (SDK)。

这些示例可分为以下几类：

操作

展示如何调用具体服务函数的代码节选。

有关 Amazon 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 Amazon Config 与 Amazon 开发工具包配合使用 (p. 51)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

代码示例

针对 的操作Amazon Config使用Amazon软件开发工具包

以下代码示例演示了如何执行个人操作：Amazon Config使用的操作Amazon开发工具包。这些摘录称之为 Amazon Config并且不旨在孤立运行 API。每个示例都包含一个指向 GitHub 的链接，其中包含了有关如何在上下文中设置和运行代码的说明。

以下示例仅包括最常用的操作。有关完整列表，请参阅 Amazon Config API 参考。

示例

删除Amazon Config规则使用Amazon开发工具包

以下代码示例显示如何删除Amazon Config规则。

Python

适用于 Python (Boto3) 的 SDK

Tip

要了解如何设置和运行此示例，请参阅 GitHub。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """
    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client

    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- 有关 API 详细信息，请参阅DeleteConfigRule在AmazonSDK for Python (Boto3) API 参考的 API 参考.

有关 Amazon 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 Amazon Config 与 Amazon 开发工具包配合使用 (p. 51)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

描述Amazon Config使用规则Amazon开发工具包

以下代码示例显示了如何描述：Amazon Config规则。

Python

适用于 Python (Boto3) 的 SDK

Tip

要了解如何设置和运行此示例，请参阅 GitHub。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """
    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client

    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
```

```
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name])
            rule = response['ConfigRules']
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- 有关 API 详细信息，请参阅DescribeConfigRules在AmazonSDK for Python (Boto3) API 参考的 API 参考.

有关 Amazon 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 Amazon Config 与 Amazon 开发工具包配合使用 (p. 51)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

设置Amazon Config规则使用Amazon开发工具包

以下代码示例显示了如何放置Amazon Config规则。

Python

适用于 Python (Boto3) 的 SDK

Tip

要了解如何设置和运行此示例，请参阅 GitHub。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """
    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client

    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    'ConfigRuleName': rule_name,
                    'Description': 'S3 Public Read Prohibited Bucket Rule',
                    'Scope': {
                        'ComplianceResourceTypes': [
                            'AWS::S3::Bucket',
                        ],
                    },
                    'Source': {
                        'Owner': 'AWS',
                        'SourceIdentifier': 'S3_BUCKET_PUBLIC_READ_PROHIBITED',
```

```
                },
                'InputParameters': '{}',
                'ConfigRuleState': 'ACTIVE'
            }
        )
        logger.info("Created configuration rule %s.", rule_name)
    except ClientError:
        logger.exception("Couldn't create configuration rule %s.", rule_name)
        raise
```

- 有关 API 详细信息，请参阅PutConfigRule在AmazonSDK for Python (Boto3) API 参考的 API 参考.

有关 Amazon 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 Amazon Config 与 Amazon 开发工具包配合使用 (p. 51)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

文档历史记录

下表介绍了对 Amazon Config 的文档的一些重要更改。如需对此文档更新的通知，您可以订阅 RSS 源。

- API 版本：2014-11-12
- 最新文档更新：2022 年 7 月 15 日

update-history-change	update-history-description	update-history-date
安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予其他权限 Amazon Amplify、Amazon AppConfig、Amazon AppSync、AmazonBilling ContorAmazon DataSync、Amazon Firewall Manager、Amazon Glue、Amazon IAM Identity Center (successor to Amazon Single Sign-On)(IAM Identity Center)、Amazon Elastic Container Service (Amazon ECS) Containc ElastiCache，Amazon EventBridge、亚马逊 FSX、Amazon Kinesis Data Analytics、亚马逊Location Service、面向 AManaged Streaming for Apache Kafka、亚马逊 QuickSight、Amazon Rekognition、亚马逊 RoboMaker、Amazon Simple Storage Service (Amazon S3)、Amazon Simple Email Service (Amazon SES)、EC2 有关更多信息，请参阅 。Amazon适用于 的托管策略Amazon Config.	2022 年 7 月 15 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config以记录对 Amazon Elastic Compute Cloud (Amazon EC2) 新资源类型所做的 有关更多信息，请参阅 。支持的资源类型.	2022 年 7 月 8 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config，用于记录配置更改Amazon全球加速器资源类型。有关更多信息，请参阅 。支持的资源类型.	2022 年 7 月 5 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录新Amazon 的配置更改	2022 年 6 月 29 日

	SageMaker 资源类型 有关更多信息，请参阅 。支持的资源类型.	
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录新的 Amazon Managed Streaming for Apache Kafka (Amazon MSK)、Amazon Route 53、Amazon WorkSpaces、Amazon Batch、Amazon Identity and Access Management Access Analyzer(IAM Amazer)、Amazon Database Migration Service(Amazon DMS)，Amazon Step Functions 和Elastic Load Balancing 资源类型。有关更多信息，请参阅 。支持的资源类型.	2022 年 6 月 14 日
Amazon Config 与 Amazon Security Hub (p. 290) 集成	借助此版本，您可以看到Amazon Config托管和自定义规则评估作为调查结果Amazon Security Hub. Security Hub 将规则评估转换为调查结果，从而提供有关受影响资源的更多信息，例如 Amazon 资源名称 (ARN) 和创建日期。这些发现可以与其他 Security Hub 调查结果一起查看，从而全面概述您的安全状况。有关更多信息，请参阅 。将规则评估发送到 Security Hub	2022 年 6 月 7 日
安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在为亚马逊 Athena、亚马逊Detective、亚马逊授予更多权限 GuardDuty、Amazon Macie、Amazon Simple Email Service (Amazon SES)、Amazon Glue、Amazon Resource Access Manager(Amazon RAM)，以及Amazon IAM Identity Center (successor to Amazon Single Sign-On). 有关更多信息，请参阅 。Amazon适用于 的托管策略 Amazon Config.	2022 年 5 月 31 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录新Amazon 的配置更改 SageMaker 和Amazon Step Functions资源类型 有关更多信息，请参阅 。支持的资源类型.	2022 年 5 月 26 日

的组成部分Amazon ConfigRule (p. 290)	在这个版本中，Amazon Config介绍的组成部分Amazon ConfigRule页. 本页讨论了规则定义的结构、规则元数据以及如何使用 Python 编写规则的最佳实践Amazon Config规则开发工具包 (RDK) 和Amazon Config规则开发工具包库 (RDKlib)。	2022 年 5 月 9 日
提高组织一致性包的服务限制 (p. 290)	在这个版本中，Amazon Config支持Amazon Config所有组织一致性包中每个账户的规则。有关更多信息，请参阅 Service Limits。	2022 年 5 月 6 日
安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予权限以获取有关全部或指定的Amazon CloudTrail事件数据存储 (EDS)，获取有关所有或指定的Amazon CloudFormation资源，获取 DynamoDB 加速器 (DAX) 参数组或子网组的列表，获取有关Amazon Database Migration Service(Amazon DMS) 在当前区域中用于您的账户的复制任务，并获取Amazon Organizations指定类型的。有关更多信息，请参阅 。Amazon适用于 的托管策略Amazon Config.	2022 年 4 月 7 日

Amazon Config自定义策略规则 (p. 290)	在这个版本中，Amazon Config让您创建Amazon Config自定义策略规则使用Amazon CloudFormationGard警卫)。Guard policy-as-code 允许您编写由强制执行的策略的语言Amazon Config而无需创建 Lambda 函数来管理您的自定义规则。使用 Guard 策略编写的规则可以从Amazon Config控制台或使用Amazon Config规则 API。 更新了开发人员指南中的以下页面： • Amazon Config自定义规则 • 创建Amazon Config带警卫的自定义规则 更新了以下 API： • Source (源) • CustomPolicyDetails • ConfigRuleEvaluationStatus • GetCustomRulePolicy • GetOrganizationCustomRulePolicy • OrganizationCustomPolicyRuleMetadata	2022 年 4 月 22 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config以记录对新 Amazon Emazon Emazon Emazon E SecurityConfiguration 资源类型。有关更多信息，请参阅 。支持的资源类型.	2022 年 3 月 31 日
Amazon Config与Amazon Ama CloudWatch 指标 (p. 290)	在这个版本中，Amazon Config现在支持追踪你的Amazon Config亚马逊的使用情况和成功指标 CloudWatch 中的Amazon Config控制面板控制面板页。CloudWatch metrics 是一项监控服务，它提供有关系统性能的数据，包括搜索、绘制图形和构建有关以下指标的警报的功能Amazon资源的费用。从Amazon Config仪表板，你可以看到哪些流量在推动你的Amazon Config使用情况和工作流程中发生的故障的关键指标。 更新了以下页面： • 查看Amazon Config控制面板	2022 年 3 月 29 日

Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录新Amazon 的配置更改GuardDuty 探测器资源类型。有关更多信息，请参阅 。支持的资源类型.	2022 年 3 月 24 日
安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在为授予额外权限Amazon Backup、Amazon Batch、DynamoDB mazonAmazon Database Migration Service、Amazon DynamoDB Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Kubernetes Service、Amazon EC2 GuardDuty、Amazon Key Management Service、Amazon OpsWorks，Amazon Relational Database ServiceAmazon WAFV2 和亚马逊 WorkSpaces.有关更多信息，请参阅 。Amazon 适用于 的托管策略Amazon Config.	2022 年 3 月 14 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config以记录对新 Amazon Elastic 容器注册表公共资源类型的配置更改。有关更多信息，请参阅 。支持的资源类型.	2022 年 3 月 4 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config以记录对新 Amazon 弹性计算云资源类型的配置更改。有关更多信息，请参阅 。支持的资源类型.	2022 年 2 月 28 日
中的日志记录和监控Amazon Config更新 (p. 290)	在这个版本中，Amazon Config更新监控Amazon Config和Amazon EventBridge 事件页面以替换对亚马逊的引用 CloudWatch 事件。亚马逊 EventBridge 是管理事件的首选方式。 CloudWatch 事件和 EventBridge 是相同的底层服务和 API，但 EventBridge 提供了更多功能。你在任一环境中所做的更改 CloudWatch 要么 EventBridge 将显示在每个控制台中。有关更多信息，请参阅。亚马逊 EventBridge.	2022 年 2 月 24 日

Amazon的开发工具包页面 Amazon Config (p. 290)	在这个版本中，Amazon Config介绍使用Amazon Config用一个Amazon开发工具包页.Amazon软件开发工具包 (SDK) 适用于许多常用编程语言。每个软件开发工具包都提供 API、代码示例和文档，使开发人员能够更轻松地以其首选语言构建应用程序。	2022 年 2 月 24 日
安全 IAM 角色信任策略更新 (p. 290)	在这个版本中，Amazon Config更新了 IAM 信任策略声明，以在信任策略中包含安全保护，该策略限制访问`sourceARN`和/或`sourceAccountId`(对于)Amazon Security Token Service(Amazon STS) operations. 这有助于确保 IAM 角色信任策略仅代表预期用户和场景访问您的资源。 更新了以下页面： • 将一个 IAM 信任策略添加到您的角色	2022 年 2 月 18 日
对全局资源类型记录的更改 (p. 290)	Amazon Config现在更改了新的全局资源类型的记录方式Amazon Config已启用. 全局资源类型为Amazon不需要您在创建时指定区域的资源。在此更改之前，Amazon Config在启用的所有区域中记录的全局资源类型Amazon Config. 进行此更改后，新的全局资源类型已载入Amazon Config录音将仅在商业分区的服务所在区域录制，并且Amazon GovCloud （美国西部）GovCloud 分区 现在，您只能在其主区域中查看这些新的全局资源类型的配置项，Amazon GovCloud （美国西部） 有关 2022 年 2 月之后加入的全球资源类型的主区域列表，请参阅记录所有受支持的资源类型页. 当前支持的全局资源类型`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、`AWS::IAM::U`保持不变，并且他们将继续在中启用的所有区域提供配置物品Amazon Config. 此更改只会影响 2022 年 2 月之后加入的新全球资源类型。	2022 年 2 月 18 日

安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予权限以获取有关 Elastic Beanstalk 环境的详细信息以及指定 Elastic Beanstalk 配置集的设置描述，获取 OpenSearch 或 Elasticsearch 版本，描述数据库的可用的 Amazon RDS 选项组，并获取有关 CodeDeploy 部署配置。此策略现在还授予权限以检索附加到的指定备用联系人Amazon账户，检索有关的信息Amazon Organizations策略，检索 Amazon ECR 存储库策略，检索有关已存档的Amazon Config规则，检索 Amazon ECS 任务定义系列的列表，列出指定子 OU 或账户的根或父组织单位 (OU)，并列出附加到指定目标根、组织单位或账户的策略。有关更多信息，请参阅 。Amazon适用于 的托管策略Amazon Config.	2022 年 2 月 10 日
安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予创建亚马逊的权限 CloudWatch 日志组和流，并将日志写入已创建的日志流。有关更多信息，请参阅 。Amazon适用于的托管策略Amazon Config.	2022 年 2 月 2 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config要记录配置更改Amazon CodeDeploy资源类型 有关更多信息，请参阅 。支持的资源类型.	2022 年 1 月 5 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录新Amazon 的配置更改 SageMaker 资源类型 有关更多信息，请参阅 。支持的资源类型.	2021 年 12 月 20 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录新Amazon 的配置更改 OpenSearch 服务资源类型。有关更多信息，请参阅 。支持的资源类型.	2021 年 10 月 12 日

安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予获取Amazon 的详细信息 OpenSearch 服务OpenSearch 服务）域/域，并获取特定 Amazon 关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表。此策略还授予权限以以以以以了解Amazon 的详细信息 ElastiCache 快照. 有关更多信息，请参阅 。Amazon适用于 的托管策略Amazon Config.	2021 年 9 月 8 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config以记录对新 Amazon 弹性计算云资源类型的配置更改。有关更多信息，请参阅 。支持的资源类型.	2021 年 9 月 7 日
Amazon SNS 策略更新 (p. 290)	在这个版本中，Amazon Config 在使用服务相关角色时更新 Amazon SNS 主题的 IAM 策略声明，以包含限制访问权限的安全保护`sourceARN`和/或`sourceAccountId`在主题策略中。这有助于确保 Amazon SNS 仅代表预期用户和场景访问您的资源。 更新了以下页面： • Amazon SNS 主题权限	2021 年 8 月 17 日
安全Amazon Lambda策略更新 (p. 290)	在这个版本中，Amazon Config 更新Amazon Lambda基于资源的策略Amazon Config包含安全保护的自定义规则，这些安全保护通过限制访问`sourceARN`和/或`sourceAccountId`在调用请求中。这有助于确保Amazon Lambda仅代表预期用户和场景访问您的资源。 更新了以下页面： • AWS::Config::ConfigRule • 为 制定自定义规则Amazon Config	2021 年 8 月 12 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录对 Amazon Kinesis 资源类型所做的配置更改。有关更多信息，请参阅 。支持的资源类型.	2021 年 8 月 6 日

示例Amazon Lambda的函数Amazon Config自定义规则 (p. 290)	在这个版本中，Amazon Config在中提供了 Python 示例函数示例Amazon Lambda的函数Amazon Config规则.	2021 年 7 月 29 日
安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予列出日志组的标签、列出状态机的标签以及列出所有状态机的权限。这些策略现在授予权限，获取状态机详细信息。这些策略现在还支持 Amazon EC2 系统管理器 (SSM)、亚马逊弹性容器注册表、亚马逊 FSX、Amazon Kinesis Data Firehose、Amazon Kinesis Data Firehose、Amazon MSK、Amazon Relational Database Service (Amazon RDS)、亚马逊 Route 53、亚马逊的额外权限 SageMaker，Amazon Simple NotificAmazon Database Migration Service、Amazon Global Accelerator, 和Amazon Storage Gateway. 有关更多信息，请参阅 。Amazon适用于 的托管策略Amazon Config.	2021 年 7 月 28 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config要记录配置更改Amazon Backup资源类型 有关更多信息，请参阅 。支持的资源类型.	2021 年 7 月 14 日
Amazon Config更新了托管规则 (p. 290)	在此版本中，Amazon Config 支持以下托管规则： • ssm-document-not-public • S3.account-level-public-access-blocks-周期性	2021 年 6 月 25 日
Amazon Config更新了托管规则 (p. 290)	在此版本中，Amazon Config 支持以下托管规则： • EC2instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip-已禁用	2021 年 6 月 10 日

安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予权限以以以以下Amazon Systems Manager有关 AM 访问分析器的文档和信息。这些策略现在支持额外的AmazonAmazon Kinesis、亚马逊的资源类型ElastiCache、AEMR zonAmazon Network Firewall、Amazon Route 53 和Amazon Relational Database Servic 这些权限更改允许Amazon Config调用支持这些资源类型所需的只读 API。这些策略现在还支持过滤 Lambda @Edge 函数lambda-inside-vpc Amazon Config托管规则。有关更多信息，请参阅 。Amazon适用于 的托管策略Amazon Config.	2021 年 6 月 8 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录 Amazon Elastic File System 资源类型发生的配置更改。有关更多信息，请参阅 。支持的资源类型.	2021 年 5 月 13 日
安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予允许的权限Amazon Config对 API Gateway 进行只读 GET 调用，以支持 API Gateway 的Config 规则。这些策略还添加了允许Amazon Config调用 Amazon Simple Storage Service (Amazon S3)，这些 API 是支持新的`AWS::S3::AccessPoint`资源类型。有关更多信息，请参阅 。Amazon适用于 的托管策略Amazon Config.	2021 年 5 月 10 日
Amazon Config自定义规则 (p. 290)	更新了开发人员指南中的以下页面： • 的自定义规则入门Amazon Config • 为 制定自定义规则Amazon Config	2021 年 4 月 30 日

安全更新 (p. 290)	这些区域有：`AWSConfigServiceRolePolicy`政策和`AWS_ConfigRole`策略现在授予权限以以以以以下Amazon Systems Manager指定的文档。这些策略现在还支持额外的Amazon的资源类型Amazon Backup，Amazon Elastic File System em，ElastiCache、Amazon Simple Storage Service（Amazon Kinesis 3）SageMaker、Amazon Database Migration Service和Amazon Amazon Amazon 这些权限更改允许Amazon Config调用支持这些资源类型所需的只读 API。有关更多信息，请参阅 。Amazon适用于的托管策略Amazon Config.	2021 年 4 月 14 日
分页更新 (p. 290)	在这个版本中，Amazon Config高级查询功能现在支持对包含聚合函数（如 COUNT 和 SUM）的查询进行分页。现在，您可以使用高级查询通过分页获取聚合查询的完整结果，分页之前限制为 500 行。有关更多信息，请参阅 。查询的当前配置状态Amazon资源	2022 年 3 月 26 日
区域支持 (p. 290)	在这个版本中，Amazon Config和Amazon Config亚太地区（大阪）区域现已支持规则。	2021 年 3 月 4 日
Amazon Config支持新资源类型 (p. 290)	借助此版本，您可以Amazon Config记录对Amazon Kubernetes Service 所做的配置更改。有关更多信息，请参阅 。支持的资源类型.	2021 年 2 月 25 日
KMS 加密支持 (p. 290)	在这个版本中，Amazon Config允许您对交付的对象使用基于 KMS 的加密Amazon Config用于 S3 存储桶交付。 更新了以下 API： • DeliveryChannel • PutDeliveryChannel 更新了开发人员指南中的以下页面： • KMS 密钥的权限 • 分配给的 IAM 角色权限Amazon Config	2021 年 2 月 16 日

保存的查询区域支持 (p. 290)	在此版本中，中现在支持已保存的查询Amazon GovCloud (US-East) 和Amazon GovCloud （美国西部）区域。	2021 年 2 月 15 日
高级查询区域支持 (p. 290)	在此版本中，非洲（开普敦）和欧洲（米兰）区域现在支持高级查询。有关更多信息，请参阅 。查询的当前配置状态Amazon资源.	2021 年 2 月 15 日
可通过 RSS 源获得 Amazon Config 文档历史记录通知 (p. 290)	现在，您可以通过订阅 RSS 源收到 Amazon Config 文档更新的通知。	2021 年 1 月 1 日

早期更新

下表介绍的文档发布历史记录Amazon Config在2020年12月31日之前。

更改	描述	发行日期
保存的查询支持	在这个版本中，Amazon Config允许您保存查询。保存查询后，可以对其进行搜索、复制到查询编辑器、编辑或删除查询。有关如何保存查询，请参阅???和???. 有关 API 的更多信息，请参阅 Amazon Config API 参考。 • PutStoredQuery • GetStoredQuery • ListStoredQueries • DeleteStoredQuery 另请参阅Service Limits (p. 25)。	2020 年 12 月 21 日
Amazon Config 支持 Amazon Network Firewall	借助此版本，您可以Amazon Config，用于记录配置更改Amazon Network Firewall FirewallPolicy、 RuleGroup和防火墙资源类型。有关更多信息，请参阅支持的资源类型 (p. 7)。	2020 年 12 月 4 日
Amazon Config 更新了托管规则	在此版本中，Amazon Config 支持以下托管规则： • iam-customer-policy-blocked-kms-actions (p. 156) • iam-inline-policy-blocked-kms-actions (p. 157)	2020 年 9 月 17 日
Amazon Config支持Amazon WAFv2	借助此版本，您可以Amazon Config，用于记录配置更改Amazon WAFv2 WebACL、IPset、 RegexPatternSet、RuleGroup, 和 ManagedRuleSet 资源类	2020 年 9 月 1 日

更改	描述	发行日期
	型 有关更多信息，请参阅 支持的资源类型 (p. 7)。	
文档更新	已添加到向 Amazon Config 用户授予自定义权限 (p. 227)关于创建授予完全访问权限的自定义权限。 文档已更新，其中包含以下规则： • s3-bucket-server-side-encryption-已启用 (p. 177) • ec2-instance-detailed-monitoring-enabled (p. 142) • ec2-managedinstance-platform-check (p. 146)	2020 年 8 月 24 日
文档更新	添加了关系查询示例。有关更多信息，请参阅 ???。	2020 年 7 月 30 日
Amazon Config支持AmazonSystems Manager	借助此版本，您可以Amazon Config，用于记录配置更改AmazonSystems Manager 文件数据资源类型。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2020 年 7 月 9 日
Amazon Config 更新了托管规则	在此版本中，Amazon Config 支持以下托管规则： • alb-http-drop-invalid-已启用标头 (p. 127) • cloudtrail-security-trail-enabled (p. 131) • cw-loggroup-retention-period-check (p. 136) • dynamodb-in-backup-plan (p. 139) • ebs-in-backup-plan (p. 141) • ec2-imdsv2-check (p. 142) • efs-in-backup-plan (p. 148) • eks-endpoint-no-public-访问 (p. 149) • eks-secrets-encrypted (p. 149) • elb-cross-zone-load-已启用平衡 (p. 151) • elb-tls-https-listeners-仅限 (p. 153) • iam-no-inline-policy-Check (p. 157) • rds-in-backup-plan (p. 166) • rds-instance-deletion-protection-已启用 (p. 165) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2020 年 7 月 9 日

更改	描述	发行日期
高级查询区域支持	在此版本中，亚太地区（香港）和中东（巴林）区域现在支持高级查询。有关更多信息，请参阅 ???。	2020 年 7 月 1 日
文档更新	文档已更新，其中包含以下规则： • ec2-managedinstance-association-compliance-status-Check (p. 145) • iam-policy-no-statements-with-admin-access (p. 159) • required-tags (p. 170) • restricted-common-ports (p. 171) • rds-snapshots-public-prohibited (p. 167) • s3-bucket-policy-grantee-check (p. 174)	2020 年 6 月 30 日
文档更新	文档已使用有关 Amazon Config 的安全的信息进行更新。请参阅 Amazon Config 中的安全性 (p. 215)。	2020 年 6 月 24 日
Amazon Config 更新了托管规则	在此版本中，Amazon Config 支持以下托管规则： • dynamodb-pitr-enabled (p. 139) • dynamodb-table-encrypted-kms (p. 140) • ec2-ebs-encryption-by-default (p. 142) • rds-snapshot-encrypted (p. 167) • redshift-require-tls-ssl (p. 169) • s3-bucket-default-lock-enabled (p. 173) • s3-default-encryption-kms (p. 178) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2020 年 5 月 28 日
Amazon Config规则区域支持	在这个版本中，很少Amazon Config非洲（开普敦）和欧洲（米兰）区域支持规则。有关规则及支持它们的区域的详细列表，请参阅Amazon Config 托管规则的列表 (p. 123)。	2020 年 4 月 28 日
Amazon Config支持AmazonSecrets Manager	借助此版本，您可以Amazon Config以记录对您的 Secrets Secrets Manager gaingain 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2020 年 4 月 20 日

更改	描述	发行日期
Amazon Config 更新了托管规则	在此版本中，Amazon Config 支持以下托管规则： • secretsmanager-rotation-enabled-check (p. 178) • secretsmanager-scheduled-rotation-success-check (p. 179) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2020 年 4 月 16 日
文档更新	Amazon Config 限制在本开发人员指南中提供。有关更多信息，请参阅 Service Limits (p. 25)。	2020 年 4 月 8 日
文档更新	自动在 Amazon Config 中将通过 Amazon CloudFormation 注册表管理（即创建/更新/删除）的第三方资源作为配置项自动跟踪。有关更多信息，请参阅记录第三方资源的配置 (p. 84)。	2020 年 3 月 30 日
文档更新	这些区域有：Amazon Config托管规则将更新以包含Amazon Web Services 区域信息。有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2020 年 3 月 27 日
Amazon Config支持 Amazon SNS 资源类型	借助此版本，您可以Amazon Config以记录您的 Amazon SNS 主题的配置更改。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2020 年 3 月 6 日
高级查询区域支持	在此版本中，欧洲（斯德哥尔摩）区域现在支持高级查询。有关更多信息，请参阅 ???。	2020 年 3 月 5 日
Amazon Config支持 Amazon SQS 资源类型	借助此版本，您可以Amazon Config以记录您的 Amazon SQS 队列的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2020 年 2 月 13 日

更改	描述	发行日期
Amazon Config 更新了托管规则	在此版本中，Amazon Config 支持以下托管规则： • api-gw-execution-logging-已启用 (p. 128) • ec2-stopped-instance (p. 147) • elasticache-redis-cluster-automatic-备份检查 (p. 150) • emr-master-no-public-ip (p. 154) • rds-enhanced-monitoring-enabled (p. 165) • s3-account-level-public-access-块 (p. 172) • service-vpc-endpoint-enabled (p. 179) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2019 年 12 月 20 日
记录自定义资源类型的配置记录	在此发行版中，Amazon Config 引入了对记录自定义资源类型的配置的支持。您可以使用 Amazon Config 控制台和 API，将第三方资源的配置数据发布到 Amazon Config 中并查看和监控资源清单及配置历史记录。有关更多信息，请参阅 记录第三方资源的配置 (p. 84)。 有关 API 的更多信息，请参阅 Amazon Config API 参考。 • DeleteResourceConfig • PutResourceConfig	2019 年 11 月 20 日
Amazon Config 支持Amazon OpenSearch 服务和Amazon Key Management Service资源类型	借助此版本，您可以Amazon Config 记录您的Amazon 发生的配置更改 OpenSearch 服务域和Amazon Key Management ServiceKey. 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2019 年 11 月 11 日
Amazon Config 更新了托管规则	在此版本中，Amazon Config 支持以下托管规则： • dms-replication-not-public (p. 138) • emr-kerberos-enabled (p. 153) • internet-gateway-authorized-vpc-限 (p. 163) • kms-cmk-not-scheduled-for delete (p. 163) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2019 年 10 月 10 日

更改	描述	发行日期
Amazon Config支持 Amazon RDS 资源类型	借助此版本，您可以Amazon Config记录对 Amazon Relational Database Service (Amazon RDS) DBClustClusterSnapshot. 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2019 年 9 月 17 日
Amazon Config 支持 Amazon QLDB 资源类型	借助此版本，您可以使用 Amazon Config 来记录对 Amazon Quantum Ledger Database (QLDB) 分类帐资源类型所做的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2019 年 9 月 10 日
Amazon Config能让您对由评估的不合规资源应用 auto 修正Amazon ConfigRule	在这个版本中，Amazon Config引入了对使用应用auto 修复的支持Amazon Systems Manager由评估的不合规资源的自动化文档Amazon Config规则。有关更多信息，请参阅 修正不合规Amazon资源 Amazon Config Rules (p. 211)。 在此版本中，Amazon Config 添加了以下新 API。有关更多信息，请参阅 Amazon Config API 参考： • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	2019 年 9 月 5 日
Amazon Config 更新了托管规则	在此版本中，Amazon Config 支持以下托管规则： • alb-http-to-https-重定向检查 (p. 127) • api-gw-cache-enabled和加密 (p. 128) • api-gw-endpoint-type-Check (p. 128) • cloudtrail-s3-dataevents-enabled (p. 130) • ebs-snapshot-public-restorable-Check (p. 141) • elb-deletion-protection-enabled (p. 152) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2019 年 8 月 22 日

更改	描述	发行日期
Amazon Config 更新了托管规则	在此版本中，Amazon Config 更新了以下托管规则： • ec2-instance-no-public-ip (p. 143) • ec2security-group-attached-to-eni (p. 147) • elasticsearch-in-vpc-only (p. 150) • redshift-cluster-public-access-check (p. 169) • vpc-sg-open-only-to-authorized-ports (p. 181) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2019 年 7 月 31 日
Amazon Config支持 Amazon EC2 资源类型	借助此版本，您可以Amazon Config记录对以下 Amazon EC2 资源所做的配置更改：VPCEndpoint、VPCEndpointService和VPCPeeringConnection. 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2019 年 7 月 12 日
Amazon Config 允许您跨组织内的所有 Amazon 账户管理 Amazon Config 规则	在此版本中，Amazon Config 支持跨组织内的所有 Amazon 账户管理 Amazon Config 规则。您可以跨组织内的所有账户集中创建、更新和删除 Amazon Config 规则。有关更多信息，请参阅 跨组织内的所有账户启用 Amazon Config 规则 (p. 209)。 有关 API 的更多信息，请参阅 Amazon Config API 参考。 • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule	2019 年 7 月 9 日
Amazon Config支持 Amazon S3 和 Amazon EC2 资源类型	借助此版本，您可以Amazon Config记录对 Amazon S3 的配置更改 AccountPublicAccessBlock 资源和以下 Amazon EC2 资源； NatGateway、EgressOnlyInternetGateway, 和 FlowLog. 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2019 年 5 月 17 日

更改	描述	发行日期
Amazon Config 允许您使用删除修正操作Amazon Web Services Management Console.	在此版本中，Amazon Config 支持使用 Amazon Web Services Management Console 删除修正操作。有关更多信息，请参阅 修正不合规Amazon资源Amazon Config Rules (p. 211)。	2019 年 4 月 24 日
Amazon Config 支持Amazon API Gateway	借助此版本，您可以Amazon Config 记录对以下 Amazon API Gateway 资源的配置更改；Api (WebSocket API)， RestApi (REST API)、Stage (WebSocket API 阶段）和阶段（REST API 阶段）。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2019 年 3 月 20 日
Amazon Config 允许您运行高级查询	在此版本中，Amazon Config 增加了对基于资源配置属性运行高级查询的支持。有关更多信息，请参阅 ???。 在此版本中，Amazon Config 增加了 `SelectResourceConfig` API。有关更多信息，请参阅 。SelectResourceConfig中的Amazon ConfigAPI 参考：	2019 年 3 月 19 日
Amazon Config 允许您将标签分配到您的 Amazon Config 资源	在这个版本中，Amazon Config引入了对三种基于标签的访问控制的支持Amazon Config资源—`ConfigRule`, `ConfigurationAggregator`,和`AggregationAuthorization`.有关更多信息，请参阅 标记您的Amazon Config 资源 (p. 90)。 在此版本中，您可以使用以下 API 从您的 Amazon Config 资源中添加、删除或列出标签。有关更多信息，请参阅 Amazon Config API 参考： • ListTagsForResource • TagResource • UntagResource	2019 年 3 月 14 日

更改	描述	发行日期
Amazon Config能让您对由评估的不合规资源应用修正Amazon ConfigRule	在这个版本中，Amazon Config引入了对使用应用补救的支持Amazon Systems Manager由评估的不合规资源的自动化文档Amazon Config规则。有关更多信息，请参阅 修正不合规Amazon资源Amazon Config Rules (p. 211)。 在此版本中，Amazon Config 添加了以下新 API。有关更多信息，请参阅 Amazon Config API 参考： • DeleteRemediationConfiguration • DescribeRemediationConfigurations • DescribeRemediationExecutionStatus • PutRemediationConfigurations • StartRemediationExecution	2019 年 3 月 12 日

更改	描述	发行日期
Amazon Config 在中国（宁夏）区域支持 Amazon Config 规则	此版本在中国（宁夏）区域中仅支持 54 个 Amazon Config 规则。有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。 但是，Amazon Config 目前在中国（宁夏）区域不支持以下规则： • acm-certificate-expiration-check • cmk-backing-key-rotation已启用 • cloudformation-stack-drift-detection-检查检查 • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-已启用验证 • codebuild-project-envvar-awscred-检查检查 • codebuild-project-source-repo-url-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-enabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-检查检查 • fms-webacl-rulegroup-association-检查检查 • guardduty-enabled-centralized • lambda-function-public-access-禁止 • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-enabled • root-account-mfa-enabled • S3.bucket-blacklisted-actions-prohibited • S3.bucket-policy-grantee-check • S3.bucket-policy-not-more-perations • S3.bucket-public-read-prohibited • S3.bucket-public-write-prohibited • S3.bucket-server-side-encryption已启用 • S3.bucket-ssl-requests-only	2019 年 3 月 12 日

更改	描述	发行日期
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • iam-user-mfa-enabled (p. 161) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2019 年 1 月 21 日
Amazon Config 支持 Amazon Service Catalog 资源类型	借助此版本，您可以Amazon Config记录对以下内容所做的配置更改Amazon Service Catalog资源； CloudFromation产品、预配置产品和产品组合。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2019 年 1 月 11 日
服务相关 Amazon Config 规则支持	在这个版本中，Amazon Config添加了一个新的托管配置规则，该规则支持其他Amazon要创建的服务Amazon Config您账户中的规则。有关更多信息，请参阅 服务相关联Amazon ConfigRule (p. 235)。	2018 年 11 月 20 日
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • access-keys-rotated (p. 126) • cloud-trail-cloud-watch-logs 已启用 (p. 133) • cloud-trail-encryption-enabled (p. 134) • cloud-trail-log-file-已启用验证 (p. 134) • iam-policy-no-statements-with-admin-access (p. 159) • iam-role-managed-policy-Check (p. 160) • iam-root-access-key-check (p. 160) • iam-user-unused-credentials-Check (p. 162) • mfa-enabled-for-iam-控制台访问权限 (p. 164) • multi-region-cloudtrail-enabled (p. 164) • vpc-flow-logs-enabled (p. 180) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2018 年 11 月 12 日

更改	描述	发行日期
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • elb-logging-enabled (p. 152) • rds-instance-public-access-Check (p. 166) • vpc-default-security-group-Close (p. 180) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2018 年 10 月 24 日
合规性历史记录支持	在此版本中，Amazon Config 现在支持存储由 Amazon Config 规则评估的资源的合规性历史记录。有关更多信息，请参阅查看资源合规性历史时间线 (p. 66)。	2018 年 10 月 18 日
Amazon Config 对 Amazon Config 规则 API 操作支持资源级权限	在此版本中，Amazon Config 对某些 Amazon Config 规则 API 操作支持资源级权限。有关支持的 API 的更多信息，请参阅Amazon Config Rules API 操作支持的资源级权限 (p. 232)。	2018 年 10 月 1 日
Amazon Config支持 CodePipeline 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon CodePipeline 资源类型所做的配置更改。有关更多信息，请参阅支持的资源类型 (p. 7)。	2018 年 9 月 12 日
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • ec2-instance-managed-by-systems-Manager (p. 143) • ec2-managedinstance-association-compliance-status-Check (p. 145) • ec2-managedinstance-patch-compliance-status-Check (p. 146) • rds-snapshots-public-prohibited (p. 167) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2018 年 9 月 5 日
Amazon Config支持AmazonSystems Manager	借助此版本，您可以Amazon Config，用于记录配置更改AmazonSystems Manager 补丁合规性和关联合规性资源类型。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2018 年 8 月 9 日

更改	描述	发行日期
Amazon Config 可让您使用 Amazon Web Services Management Console删除 Amazon Config 数据	在此版本中，Amazon Config 使用 Amazon Web Services Management Console引入了对保留期的支持。在 Amazon Web Services Management Console中，您可以为 `ConfigurationItems` 选择自定义数据保留期。有关更多信息，请参阅 删除Amazon Config数据 (p. 82)。	2018 年 8 月 7 日
Amazon Config 支持 Amazon Shield 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon Shield 保护资源类型所做的配置更改。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2018 年 8 月 7 日
Amazon Config 支持Amazon PrivateLink	在这个版本中，Amazon Config支持 Amazon PrivateLink，能让您在 Amazon Virtual Private Cloud (VPC) 和Amazon Config完全在Amazon网络的 有关更多信息，请参阅 使用Amazon Config使用 Amazon VPC 终端节 (p. 277)。	2018 年 7 月 31 日
Amazon Config 可让您删除 Amazon Config 数据	在此版本中，Amazon Config 引入了对保留期的支持。Amazon Config 可让您通过为 `ConfigurationItems` 指定保留期来删除数据。有关更多信息，请参阅 删除Amazon Config数据 (p. 82)。 在此版本中，Amazon Config 添加了以下新 API。有关更多信息，请参阅 Amazon Config API 参考： • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	2018 年 5 月 25 日
Amazon Config 支持新的托管规则	此版本支持以下两新的托管规则： • s3-bucket-replication-enabled (p. 176) • iam-policy-blacklisted-check (p. 158) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2018 年 5 月 10 日
Amazon Config 支持 Amazon X-Ray 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon X-Ray EncryptionConfig 资源类型所做的配置更改。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2018 年 5 月 1 日
Amazon Config 支持 Amazon Elastic Beanstalk 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon Elastic Beanstalk 应用程序、应用程序版本和环境资源所做的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2018 年 24 月 4 日

更改	描述	发行日期
监控Amazon Config和Amazon CloudWatch 事件	在此版本中，使用亚马逊 CloudWatch 事件以检测状态的变更并对其进行响应 Amazon Config事件. 有关更多信息，请参阅 监控 Amazon Config和 Amazon EventBridge (p. 275)。	2018 年 3 月 29 日
新的 API 操作	在这个版本中，Amazon Config增加了对的支持BatchGetResourceConfigAPI，能让您批量检索一个或多个资源的当前状态。	2018 年 3 月 20 日
Amazon Config 支持 Amazon WAF RuleGroup 资源类型	借助此版本，您可以Amazon Config，用于记录配置更改AmazonWAF RuleGroup和AmazonWAF RuleGroup 区域资源。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2018 年 2 月 15 日
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • elb-custom-security-policy-ssl-check (p. 151) • elb-predefined-security-policy-ssl-check (p. 152) • iam-group-has-users-Check (p. 156) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2018 年 1 月 25 日
Amazon Config 支持Elastic Load Bcing	借助此版本，您可以使用 Amazon Config 来记录对 Elastic Load Balancing 传统负载均衡器所做的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2017 年 11 月 17 日
Amazon Config支持Amazon Ama CloudFront 和 Amazon WAF资源类型	借助此版本，您可以Amazon Config，用于记录配置更改 CloudFront 分布和流分配。 在此版本中，您可以使用 Amazon Config 记录对以下 Amazon WAF 和 Amazon WAF 区域资源所做的配置更改：基于速率的规则、规则和 Web ACL。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2017 年 11 月 15 日
Amazon Config 支持 Amazon CodeBuild 资源类型	在此版本中，您可以使用 Amazon Config 记录对您的 Amazon CodeBuild 项目所做的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2017 年 10 月 20 日

更改	描述	发行日期
Amazon Config支持 Auto Scaling 资源和一条新的托管规则	借助此版本，您可以Amazon Config记录对以下 Auto Scaling 资源所做的配置更改：组、启动配置、计划操作和扩展策略。 有关更多信息，请参阅 支持的资源类型 (p. 7)。 此版本还支持以下托管规则： • autoscaling-group-elb-healthcheck-必需 (p. 130) 有关更多信息，请参阅 Amazon Config 托管规则 (p. 123)。	2017 年 9 月 18 日
Amazon Config 支持 Amazon CodeBuild 资源类型	在此版本中，您可以使用 Amazon Config 记录对您的 Amazon CodeBuild 项目所做的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2017 年 10 月 20 日
Amazon Config支持 Auto Scaling 资源和一条新的托管规则	借助此版本，您可以Amazon Config记录对以下 Auto Scaling 资源所做的配置更改：组、启动配置、计划操作和扩展策略。 有关更多信息，请参阅 支持的资源类型 (p. 7)。 此版本还支持以下托管规则： • autoscaling-group-elb-healthcheck-必需 (p. 130) 有关更多信息，请参阅 Amazon Config 托管规则 (p. 123)。	2017 年 9 月 18 日
Amazon Config支持 DynamoDB 表资源类型和一条新的托管规则	借助此版本，您可以Amazon Config以记录对您的 DynamoDB 表所做的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。 此版本支持以下托管规则： • dynamodb-autoscaling-enabled (p. 138) 有关更多信息，请参阅 Amazon Config 托管规则 (p. 123)。	2017 年 9 月 8 日

更改	描述	发行日期
Amazon Config 控制台中的新页面	您可以使用 控制台中的 DashboardAmazon Config 来查看以下内容： • 资源总数 • 规则总数 • 不合规资源数 • 不合规规则数 有关更多信息，请参阅 查看 Amazon Config 控制面板 (p. 56)。	2017 年 7 月 17 日
新的 API 操作	您可以使用GetDiscoveredResourceCounts操作以返回资源类型数、每个资源类型的数量，以及总资源数Amazon Config正在为你录制一个区域Amazonaccount.	2017 年 7 月 17 日
Amazon Config 支持 Amazon CloudFormation 堆栈资源类型和一条新的托管规则	在此版本中，您可以使用 Amazon Config 记录对您的 Amazon CloudFormation 堆栈所做的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2017 年 6 月 7 日
新增和更新的内容	此版本增加了对的支持Amazon Config加拿大（中部）区域和南美洲（圣保罗）区域的规则。 适用于支持的所有区域Amazon Config和Config 规则，请参阅Amazon Web Services 区域和终端节点中的Amazon一般参考.	2017 年 5 月 7 日
新增和更新的内容	Amazon Config 规则在Amazon GovCloud (US)区域中可用。有关更多信息，请参阅《Amazon GovCloud (US) 用户指南》。 对于支持Amazon Config，请参阅Amazon Web Services 区域和终端节点中的Amazon一般参考.	2017 年 6 月 8 日

更改	描述	发行日期
Amazon Config支持Amazon Ama CloudWatch 警报资源类型和三个新托管规则	借助此版本，您可以Amazon Config记录您的Amazon 发生的配置更改 CloudWatch 警报。 有关更多信息，请参阅 支持的资源类型 (p. 7)。 此版本支持三条新的托管规则： • cloudwatch-alarm-action-check (p. 131) • cloudwatch-alarm-resource-check (p. 132) • cloudwatch-alarm-settings-check (p. 133) 有关更多信息，请参阅 Amazon Config 托管规则 (p. 123)。	2017 年 6 月 1 日
新增和更新的内容	此版本支持为以下托管规则指定应用程序版本号： • ec2-managedinstance-applications-blacklisted (p. 144) • ec2-managedinstance-applications-required (p. 144) 有关更多信息，请参阅 Amazon Config 托管规则 (p. 123)。	2017 年 6 月 1 日
新增和更新的内容	此版本增加了对的支持Amazon Config亚太地区（孟买）区域的规则。有关更多信息，请参阅 。Amazon Web Services 区域和终端节点中的Amazon一般参考.	2017 年 4 月 27 日
新增和更新的内容	此版本支持更新的控制台体验，可让您首次将 Amazon Config 托管规则添加到您的账户。 当您首次设置 Amazon Config 规则或者在新区域中设置这些规则时，您可以按名称、描述或标签搜索 Amazon 托管规则。您可以选择 Select all 以选择所有规则，或者选择 Clear all 以清除所有规则。 有关更多信息，请参阅 使用Amazon Config控制台规则 (p. 52)。	2017 年 4 月 5 日

更改	描述	发行日期
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • ec2-instance-detailed-monitoring-enabled (p. 142) • ec2-managedinstance-inventory-blacklisted (p. 145) • ec2-volume-inuse-check (p. 147) • iam-user-group-membership-check (p. 161) • iam-user-no-policies-Check (p. 162) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2017 年 2 月 21 日
新增和更新的内容	此版本增加了对的支持Amazon Config欧洲（伦敦）区域的规则。有关更多信息，请参阅 。Amazon Web Services 区域和终端节点中的Amazon一般参考.	2017 年 2 月 21 日
新增和更新的内容	此版本增加了适用于 Amazon Config 托管规则的 Amazon CloudFormation 模板。您可以使用这些模板为您的账户创建托管规则。有关更多信息，请参阅 使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则 (p. 182)。	2017 年 2 月 16 日
新增和更新的内容	此版本增加了对 `PutEvaluations` API 的新测试模式的支持。在自定义规则中将 `TestMode` 参数设置为 true 以验证 Amazon Lambda 函数是否将评估结果传送到 Amazon Config。不会更新现有评估，并且不会将评估结果发送到 Amazon Config。 有关更多信息，请参阅 。PutEvaluations中的Amazon ConfigAPI 参考.	2017 年 2 月 16 日
新增和更新的内容	此版本增加了对的支持Amazon Config亚太地区（首尔）和美国西部（加利福利亚北部）区域的规则。有关更多信息，请参阅 。Amazon Web Services 区域和终端节点中的Amazon一般参考.	2016 年 12 月 21 日
新增和更新的内容	此版本增加了对的支持Amazon Config在欧洲（伦敦）区域。有关更多信息，请参阅 。Amazon Web Services 区域和终端节点中的Amazon一般参考.	2016 年 12 月 13 日
新增和更新的内容	此版本增加了对的支持Amazon Config在加拿大（中部）区域。有关更多信息，请参阅 。Amazon Web Services 区域和终端节点中的Amazon一般参考.	2016 年 12 月 8 日

更改	描述	发行日期
Amazon Config 支持 Amazon Redshift 资源类型和两条新的托管规则	借助此版本，您可以Amazon Config记录您的 Amazon Redshift 群集、群集安全组、群集快照、群集子网组和事件订阅的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。 此版本支持两条新的托管规则： • redshift-cluster-configuration-check (p. 168) • redshift-cluster-maintenancesettings-check (p. 168) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2016 年 12 月 7 日
新增和更新的内容	此版本增加了对新托管规则的支持： • dynamodb-throughput-limit-check (p. 140) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2016 年 12 月 7 日
新增和更新的内容	此版本增加了以下支持：可在一个账户中针对每个区域创建多达 50 条规则。有关更多信息，请参阅 。AmazonConfig中的Amazon一般参考.	2016 年 12 月 7 日
Amazon Config支持 Amazon EC2 Systems Manager 的托管实例清单资源类型，以及三种新的托管规则	您可以使用此版本的 Amazon Config 记录托管实例的软件配置变更，还支持托管实例清单。 有关更多信息，请参阅 Recording Software Configuration for Managed Instances (p. 81)。 此版本支持三条新的托管规则： • ec2-managedinstance-inventory-blacklisted (p. 145) • ec2-managedinstance-applications-required (p. 144) • ec2-managedinstance-platform-check (p. 146) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2016 年 12 月 1 日
新增和更新的内容	Amazon Config在中国（北京）区域推出。	2016 年 10 月 24 日

更改	描述	发行日期
Amazon Config支持 Amazon S3 存储桶资源和两条新的托管规则	借助此版本，您可以Amazon Config以记录您的 Amazon S3 存储桶的配置更改。有关更多信息，请参阅 支持的资源类型 (p. 7)。 此版本支持两条新的托管规则： • s3-bucket-logging-enabled (p. 173) • s3-bucket-versioning-enabled (p. 177) 有关更多信息，请参阅 Amazon Config 托管规则 (p. 123)。	2016 年 10 月 18 日
新增和更新的内容	此版本增加了对的支持Amazon Config和Amazon Config美国东部（俄亥俄州）区域的规则。有关更多信息，请参阅 。Amazon Web Services 区域和终端节点中的Amazon一般参考.	2016 年 10 月 17 日
新增和更新的管理规则	此更新添加了对八个新的管理规则的支持： • approved-amis-by-id (p. 129) • approved-amis-by-tag (p. 129) • db-instance-backup-enabled (p. 136) • desired-instance-type (p. 137) • ebs-optimized-instance (p. 141) • iam-password-policy (p. 158) • rds-multi-az-support (p. 166) 您可以为以下规则指定多个参数值： • desired-instance-tenancy (p. 137) • required-tags (p. 170) 有关更多信息，请参阅 Amazon Config 托管规则的列表 (p. 123)。	2016 年 10 月 4 日
Amazon Config 控制台的新增和更新内容	此更新增加了对在 Amazon Config 时间线中查看 Amazon CloudTrail API 活动的支持。如果 CloudTrail 是您的账户的日志记录，您可以查看、创建、更新和删除 API 事件 (针对您的资源的配置更改)。有关更多信息，请参阅 查看配置详细信息 (p. 59)。	2016 年 9 月 6 日
Amazon Config 支持Elastic Load Bcing	借助此版本，您可以Amazon Config以记录对 EElastic Load Balancing ad Balancin 应用程序负载均衡器所做的配置更改。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2016 年 8 月 31 日

更改	描述	发行日期
新增和更新的内容	此版本增加了对的支持Amazon Config亚太地区（新加坡）和亚太地区（悉尼）区域的规则。有关更多信息，请参阅 。Amazon Web Services 区域和终端节点中的Amazon一般参考.	2016 年 8 月 18 日
Amazon Config 规则的新增和更新内容	此更新增加了支持，用以创建一个既可按配置更改触发、又可按您选择的定期频率触发的规则。有关更多信息，请参阅 为 Amazon Config 规则指定触发器 (p. 122)。 此更新还增加了支持，用以手动按照规则评估您的资源和删除评估结果。有关更多信息，请参阅 评估您的资源 (p. 208)。 此更新还增加了支持，用以使用自定义规则来评估其他资源类型。有关更多信息，请参阅 评估其他资源类型 (p. 191)。	2016 年 7 月 25 日
Amazon Config 支持 Amazon AmazonAmazon Certificate Manager(ACM) 资源类型	借助此版本，您可以Amazon Config记录您的 Amazon Relational Database Service (Amazon RDS) 数据库实例、数据库安全组、数据库快照、数据库子网组和事件订阅的配置更改。您还可以使用Amazon Config以记录由 ACM 提供的证书的配置更改。 有关更多信息，请参阅 支持的资源类型 (p. 7)。	2016 年 7 月 21 日
有关管理配置记录器的更新信息	此更新增加了步骤，用以重命名和删除管理配置记录器 (p. 79) 的配置记录器。	2016 年 7 月 7 日
简化的角色创建过程和更新策略	通过此更新，为创建 IAM 角色Amazon Config被简化了。支持 Config 规则的区域中均提供了此增强功能。为支持此增强功能，使用控制台设置 Amazon Config (p. 27) 中的步骤、Amazon S3 存储桶的权限 (p. 221) 中的示例策略及向 Amazon Config 用户授予自定义权限 (p. 227) 中的示例策略均已进行更新。	2016 年 3 月 31 日
Config 规则的示例函数和事件	此更新在 用于 Amazon Config 规则 (Node.js) 的示例 Amazon Lambda 函数 (p. 192) 中提供了更新的示例函数，并在 Amazon Config 规则的示例事件 (p. 202) 中添加了示例事件。	2016 年 3 月 29 日
Amazon ConfigRule GitHub 知识库	此更新添加了有关的信息Amazon ConfigRule GitHub 知识库到使用 Amazon Config 规则评估资源 (p. 105). 此存储库提供了 Amazon Config 用户开发和贡献的自定义规则的示例函数。	2016 年 3 月 1 日

更改	描述	发行日期
Amazon Config 规则	此版本介绍了 Amazon Config 规则。借助规则，您可以使用 Amazon Config 评估您的 Amazon 资源是否符合您所需的配置。有关更多信息，请参阅 使用 Amazon Config 规则评估资源 (p. 105)。	2015 年 12 月 18 日
Amazon Config支持 IAM 资源类型	借助此版本，您可以Amazon Config记录对 IAM 用户、组、角色和客户托管策略所做的配置更改。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2015 年 12 月 10 日
Amazon Config 支持 EC2 专用主机	借助此版本，您可以使用 Amazon Config 记录您的 EC2 专用主机的配置更改。有关更多信息，请参阅 支持的资源类型 (p. 7)。	2015 年 11 月 23 日
更新的权限信息	此更新添加了有关 Amazon Config 的下列 Amazon 托管策略的信息： • `AWS_ConfigRole`— 授予Amazon Config权限以获取您的资源的配置详细信息。有关更多信息，请参阅 用于获取配置详细信息的 IAM 角色策略 (p. 220)。 • `AWSConfigUserAccess`-授予对的只读访问权限Amazon Config用户。有关更多信息，请参阅 向 Amazon Config 用户授予自定义权限 (p. 227)。	2015 年 10 月 19 日
Amazon Config 规则预览	此版本介绍了 Amazon Config 规则预览。借助规则，您可以使用 Amazon Config 评估您的 Amazon 资源是否符合您所需的配置。有关更多信息，请参阅 使用 Amazon Config 规则评估资源 (p. 105)。	2015 年 10 月 7 日
新增和更新的内容	此版本增加了查找 Amazon Config 发现的资源的功能。有关更多信息，请参阅 查找 Amazon Config 发现的资源 (p. 58)。	2015 年 8 月 27 日
新增和更新的内容	此版本增加了选择 Amazon Config 记录哪些类型资源的功能。有关更多信息，请参阅 选择 Amazon Config 所记录的资源 (p. 73)。	2015 年 6 月 23 日
新增和更新的内容	此版本增加了对以下区域的支持：亚太地区（东京）、亚太地区（新加坡）、南美洲（圣保罗）和美国西部（加利福利亚北部）。有关更多信息，请参阅Amazon Web Services 区域 和端点。	2015 年 4 月 6 日
新指南	此版本引入了 Amazon Config。	2014 年 11 月 12 日

Amazon词汇表

有关最新Amazon术语，请参阅《Amazon一般参考》中的Amazon术语表。

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。