
AWS Config

开发人员指南



AWS Config: 开发人员指南

Copyright © 2018 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

什么是 AWS Config ?	1
AWS Config 的使用方式	1
资源管理	1
审计与合规性	1
对配置更改进行管理与故障排除	1
安全分析	1
概念	2
AWS Config 规则	2
AWS 资源	2
配置历史	2
配置项	3
配置记录器	3
配置快照	3
配置流	3
资源关系	3
多账户多区域数据聚合	3
AWS Config 的工作原理 ?	4
传送配置项	4
支持的资源、配置项和关系	6
支持的 AWS 资源类型	6
记录托管实例的软件配置	8
配置项的组成部分	9
支持的资源关系	11
入门	15
注册 AWS	15
使用控制台设置 AWS Config	15
使用控制台设置 AWS Config	17
使用 AWS CLI 设置 AWS Config	19
先决条件	19
启用 AWS Config	22
验证 AWS Config 是否打开	22
查看 AWS Config 控制面板	24
使用规则评估资源	26
为 AWS Config 规则指定触发器	26
触发器类型	26
具有触发器的规则示例	27
关闭配置记录器时的规则评估	27
关于 AWS 托管 Config 规则	28
AWS 托管配置规则	28
使用 AWS 托管规则	55
使用 AWS CloudFormation 模板创建 AWS Config 托管规则	56
为 AWS Config 制定自定义规则	56
自定义规则入门	57
制定自定义规则	59
函数和事件示例	62
查看配置合规性	69
管理您的 AWS Config 规则	72
使用控制台	72
使用 AWS CLI	74
使用 AWS Config API	75
删除评估结果	76
手动评估您的资源	76
评估您的资源	76
删除评估结果	77

查看 AWS 资源配置和历史记录	78
查找已发现的资源	78
查找资源 (AWS Config 控制台)	78
查找资源 (AWS CLI)	78
查找资源 (AWS Config API)	79
在控制台中查看配置详细信息	79
使用 CLI 查看配置详细信息	81
查看配置历史记录	81
传送配置快照	82
示例 Amazon EBS 配置历史记录	83
配置快照示例	86
AWS Config 发送的通知	90
通过邮件电子监控资源变更	90
示例配置项变更通知	94
示例配置历史记录传输通知	101
示例配置快照传输开始通知	102
示例配置快照传输通知	102
示例合规性变更通知	103
示例规则评估开始通知	104
示例过大配置项变更通知	105
示例传输失败通知	105
多账户多区域数据聚合	107
设置聚合器 (控制台)	107
添加聚合器	108
编辑聚合器	109
删除聚合器	109
了解更多	109
设置聚合器 (AWS CLI)	109
使用个人账户添加聚合器	110
使用 AWS 组织添加聚合器	111
查看聚合器	111
编辑聚合器	112
删除聚合器	113
了解更多	109
授权聚合器账户 (控制台)	113
为聚合器账户和区域添加授权	114
授权针对聚合器账户的待处理请求	114
删除对现有聚合器账户的授权	115
了解更多	109
授权聚合器账户 (AWS CLI)	115
为聚合器账户和区域添加授权	115
删除授权账户	116
了解更多	109
在聚合视图中查看合规性数据	116
使用聚合视图	116
了解更多	109
故障排除	118
了解更多	109
管理 AWS Config	119
管理传递通道	119
更新传递通道	119
重命名传递通道	120
更新 IAM 角色	121
更新 IAM 角色	121
管理配置记录器	122
管理配置记录器 (控制台)	122
管理配置记录器 (AWS CLI)	123

选择所记录的资源	124
记录所有受支持的资源类型	124
记录特定的资源类型	124
选择资源 (控制台)	124
选择资源 (AWS CLI)	125
权限	128
IAM 角色权限	128
创建 IAM 角色策略	128
有关记录 S3 存储桶的疑难解答	130
针对 Amazon S3 存储桶的权限	130
其他账户中的 Amazon S3 存储桶所需的权限	131
授权 AWS Config 访问其他账户中的 Amazon S3 存储桶	131
Amazon SNS 主题的权限	132
用户的权限	132
示例策略	133
监控	136
使用 Amazon SQS	136
Amazon SQS 权限	136
使用 Amazon CloudWatch Events	137
适用于 AWS Config 的 Amazon CloudWatch Events 格式	138
为 AWS Config 创建 Amazon CloudWatch Events 规则	138
使用 AWS CloudTrail 记录 AWS Config API 调用	140
CloudTrail 中的 AWS Config 信息	140
了解 AWS Config 日志文件条目	140
示例日志文件	140
DeleteDeliveryChannel	141
DeliverConfigSnapshot	141
DescribeConfigurationRecorderStatus	142
DescribeConfigurationRecorders	142
DescribeDeliveryChannels	143
GetResourceConfigHistory	143
PutConfigurationRecorder	144
PutDeliveryChannel	145
StartConfigurationRecorder	145
StopConfigurationRecorder	146
AWS Config 资源	147
适用于 AWS Config 的 AWS 开发工具包	147
文档历史记录	149
AWS 词汇表	160

什么是 AWS Config ?

AWS Config 可以提供关于您的 AWS 账户中的 AWS 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。

AWS 资源是您可以在 AWS 中使用的一种实体，例如 Amazon Elastic Compute Cloud (EC2) 实例、Amazon Elastic Block Store (EBS) 卷、安全组或 Amazon Virtual Private Cloud (VPC)。要了解 AWS Config 支持的 AWS 资源的完整列表，请参阅 [支持的 AWS 资源类型](#) (p. 6)。

利用 AWS Config，您可以：

- 评估您 AWS 资源配置是否具备所需设置。
- 获得与您的 AWS 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。

AWS Config 的使用方式

当您在 AWS 上运行应用程序时，您通常要使用 AWS 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 AWS 资源的需求也在不断增加。AWS 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。AWS 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 AWS Config 规则来评估自己的 AWS 资源的配置设置。当 AWS Config 检测到不符合某项规则所设定条件的资源时，AWS Config 会将其标记为不合规资源并向您发送通知。AWS 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。AWS 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 AWS 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 AWS 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 AWS 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，您需要了解您的 AWS 资源配置的详细历史信息，例如授予您的用户的 AWS Identity and Access Management (IAM) 权限或者控制资源访问的 Amazon EC2 安全组规则。

您可以使用 AWS Config 随时查看其正在记录的分配给 IAM 用户、组或角色的 IAM 策略。这一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 John Doe 在 2015 年 1 月 1 日是否具备修改 Amazon VPC 设置的权限。

您也可以使用 AWS 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。这一信息可以帮助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

了解 AWS Config 的基本组成部分可以帮助您充分利用这项服务。

内容

- [AWS Config 规则 \(p. 2\)](#)
- [AWS 资源 \(p. 2\)](#)
- [配置历史 \(p. 2\)](#)
- [配置项 \(p. 3\)](#)
- [配置记录器 \(p. 3\)](#)
- [配置快照 \(p. 3\)](#)
- [配置流 \(p. 3\)](#)
- [资源关系 \(p. 3\)](#)
- [多账户多区域数据聚合 \(p. 3\)](#)
 - [源账户 \(p. 3\)](#)
 - [源区域 \(p. 3\)](#)
 - [聚合器 \(p. 4\)](#)
 - [聚合器账户 \(p. 4\)](#)
 - [授权 \(p. 4\)](#)

AWS Config 规则

AWS Config 规则规定了特定 AWS 资源或整个 AWS 账户需要具备的配置设置。AWS Config 能够提供可自定义的预定义规则，以帮助您开始进行评估。您也可以创建自定义规则。AWS 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。如果某个资源不符合规则，AWS Config 会将该资源和规则标记为不合规，并通过 Amazon SNS 通知您。有关更多信息，请参阅 [使用 AWS Config 规则评估资源 \(p. 26\)](#)。

AWS 资源

AWS 资源是您使用 AWS 管理控制台、AWS Command Line Interface (CLI)、AWS SDK 或 AWS 合作伙伴工具创建和管理的实体。AWS 资源的示例包括 Amazon EC2 实例、安全组、Amazon VPC 以及 Amazon Elastic Block Store。AWS Config 用唯一的标识符来标记每个资源，例如资源 ID 或 [Amazon 资源名称 \(ARN\)](#)。有关详细信息，请参阅 [支持的 AWS 资源类型 \(p. 6\)](#)。

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。AWS Config 可以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 AWS 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

配置项代表您账户中受支持的 AWS 资源在特定时间点具备的各种属性。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，AWS Config 就会创建配置项。例如，如果 AWS Config 正在记录 Amazon S3 存储桶，则只要创建、更新或删除存储桶，AWS Config 就会创建配置项。

有关更多信息，请参阅 [配置项的组成部分 \(p. 9\)](#)。

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 \(p. 122\)](#)。

默认情况下，配置记录器会记录 AWS 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 AWS Config 所记录的资源 \(p. 124\)](#)。

如果您使用 AWS 管理控制台 或 CLI 打开服务，AWS 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 Simple Storage Service (Amazon S3) 存储桶。此外，您可以在 AWS 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 AWS 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，AWS 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 AWS 资源配置的外部系统。

资源关系

AWS Config 会查找您账户中的 AWS 资源，然后创建 AWS 资源关系图。例如，Amazon EBS 卷 vol-123ab45d 挂载到 Amazon EC2 实例 i-a1b2c3d4，而该实例又与安全组 sg-ef678hk 关联，这就构成了一种关系。

有关更多信息，请参阅 [支持的资源关系 \(p. 11\)](#)。

多账户多区域数据聚合

AWS Config 中多账户多区域数据聚合能让您从多个账户和区域将 AWS Config 数据聚合到单个账户中。多账户多区域数据聚合用于让中心 IT 管理员监控企业中多个 AWS 账户的合规性。

源账户

源账户是您要从中聚合 AWS Config 资源配置和合规性数据的 AWS 账户。源账户可以是 AWS Organizations 中的个人账户或组织。您可以单独提供源账户，也可以通过 AWS Organizations 检索它们。

源区域

源区域是您要从中聚合 AWS Config 数据的 AWS 区域。

聚合器

聚合器是 AWS Config 中的一种新的资源类型，用于从多个源账户和区域收集 AWS Config 数据。在要查看聚合 AWS Config 数据的区域中创建聚合器。

聚合器账户

聚合账户是您在其中创建聚合器的账户。

授权

作为源账户所有者，授权是指您向聚合账户和区域授予收集 AWS Config 数据的权限。如果要聚合的源账户是 AWS Organizations 的一部分，则不需要授权。

有关更多信息，请参阅 [Multi-Account Multi-Region Data Aggregation \(p. 107\)](#)。

AWS Config 的工作原理？

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

AWS 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，AWS Config 会为区域内每个支持的资源创建配置项。如果您不希望 AWS 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。

AWS 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 AWS Config 对安全组调用 Describe API。然后 AWS 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）更新后的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。

AWS Config 还会跟踪不是由 API 发起的配置更改。AWS 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 AWS Config 规则，那么 AWS Config 会持续评估您的 AWS 资源是否具备所需设置。根据具体规则，AWS 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 AWS Lambda 函数关联，其中包含规则的评估逻辑。当 AWS Config 评估您的资源时，它会调用与规则关联的 AWS 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 AWS 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，AWS Config 会向您的 Amazon SNS 主题发送通知。

传送配置项

AWS Config 可以通过以下通道传送配置项：

Amazon S3 存储桶

AWS Config 会跟踪您的 AWS 资源的配置更改，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 AWS 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，AWS Config 则不会发送文件。

当您通过 AWS CLI 使用 [deliver-config-snapshot](#) 命令时，或当您通过 AWS Config API 使用 [DeliverConfigSnapshot](#) 操作时，AWS Config 会将一个配置快照发送到您的 Amazon S3 存储桶。配置快照中包含 AWS Config 记录的、您的 AWS 账户中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

AWS Config 只将配置历史记录文件和配置快照传输到指定的 S3 存储桶；AWS Config 不修改 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 Glacier。有关更多信息，请参阅 Amazon Simple Storage Service 控制台用户指南 中的[管理生命周期配置](#)。您还可以查看[将 Amazon S3 数据存档到 Amazon Glacier](#) 博客文章。

Amazon SNS 主题

Amazon Simple Notification Service (Amazon SNS) 主题是一个通信渠道，Amazon SNS 使用它将消息（或通知）传送到订阅终端节点，例如电子邮箱地址或客户端（如 [Amazon Simple Queue Service](#) 队列）。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。

AWS 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`

AWS Config 评估的资源的合规性状态已更改。合规性类型表明资源是否符合特定 AWS Config 规则，由消息中的 `ComplianceType` 键体现。消息中包含 `newEvaluationResult` 和 `oldEvaluationResult` 对象，以便进行比较。

`ConfigRulesEvaluationStarted`

AWS Config 开始针对指定的资源评估您的规则。

`ConfigurationSnapshotDeliveryStarted`

AWS Config 开始向您的 Amazon S3 存储桶传送配置快照。Amazon S3 存储桶的名称将为消息中的 `s3Bucket` 键提供值。

`ConfigurationSnapshotDeliveryCompleted`

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

`ConfigurationSnapshotDeliveryFailed`

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

`ConfigurationHistoryDeliveryCompleted`

AWS Config 已成功将配置历史记录传送到您的 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 AWS 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了 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。您可以在指定的 Amazon S3 存储桶位置查看完整通知。

`OversizedConfigurationItemChangeDeliveryFailed`

AWS Config 无法将过大配置项变更通知传送到您的 Amazon S3 存储桶。

有关示例通知，请参阅 [AWS Config 发送的通知 \(p. 90\)](#)。

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、配置项和关系

AWS Config 支持以下 AWS 资源、配置项和资源关系。

内容

- [支持的 AWS 资源类型](#) (p. 6)
- [记录托管实例的软件配置](#) (p. 8)
- [配置项的组成部分](#) (p. 9)
 - [Amazon S3 存储桶属性](#) (p. 10)
- [支持的资源关系](#) (p. 11)

支持的 AWS 资源类型

AWS Config 支持以下 AWS 资源类型。

AWS 服务	资源类型	资源类型值
Auto Scaling	Auto Scaling 组	AWS::AutoScaling::AutoScalingGroup
	Auto Scaling 启动配置	AWS::AutoScaling::LaunchConfiguration
	Auto Scaling 扩展策略	AWS::AutoScaling::ScalingPolicy
	Auto Scaling 计划操作	AWS::AutoScaling::ScheduledAction
AWS Certificate Manager	证书	AWS::ACM::Certificate
AWS CloudFormation	堆栈 ¹	AWS::CloudFormation::Stack
Amazon CloudFront ²	分配	AWS::CloudFront::Distribution
	流分配	AWS::CloudFront::StreamingDistribution
AWS CloudTrail	试用	AWS::CloudTrail::Trail
AWS CodeBuild	项目 ³	AWS::CodeBuild::Project
Amazon CloudWatch	警报	AWS::CloudWatch::Alarm
Amazon DynamoDB	Table	AWS::DynamoDB::Table
Amazon Elastic Block Store	Amazon EBS 卷	AWS::EC2::Volume
Amazon Elastic Compute Cloud	EC2 专用主机 ⁴	AWS::EC2::Host
	EC2 弹性 IP (仅限 VPC)	AWS::EC2::EIP
	EC2 实例	AWS::EC2::Instance
	EC2 网络接口	AWS::EC2::NetworkInterface

AWS 服务	资源类型	资源类型值
	EC2 安全组	AWS::EC2::SecurityGroup
Amazon EC2 Systems Manager	托管实例清单 ⁵	AWS::SSM::ManagedInstanceInventory
Elastic Load Balancing	应用程序负载均衡器	AWS::ElasticLoadBalancingV2::LoadBalancer
	传统负载均衡器	AWS::ElasticLoadBalancing::LoadBalancer
	网络负载均衡器	AWS::ElasticLoadBalancingV2::LoadBalancer
AWS Identity and Access Management ⁶	IAM 用户 ⁷	AWS::IAM::User
	IAM 组 ⁷	AWS::IAM::Group
	IAM 角色 ⁷	AWS::IAM::Role
	IAM 客户管理的政策	AWS::IAM::Policy
Amazon Redshift	集群	AWS::Redshift::Cluster
	群集参数组	AWS::Redshift::ClusterParameterGroup
	群集安全组	AWS::Redshift::ClusterSecurityGroup
	群集快照	AWS::Redshift::ClusterSnapshot
	群集子网组	AWS::Redshift::ClusterSubnetGroup
	事件订阅	AWS::Redshift::EventSubscription
Amazon Relational Database Service	RDS 数据库实例	AWS::RDS::DBInstance
	RDS 数据库安全组	AWS::RDS::DBSecurityGroup
	RDS 数据库快照	AWS::RDS::DBSnapshot
	RDS 数据库子网组	AWS::RDS::DBSubnetGroup
	事件订阅	AWS::RDS::EventSubscription
Amazon Simple Storage Service	Amazon S3 存储桶 ⁸	AWS::S3::Bucket
Amazon Virtual Private Cloud	客户网关	AWS::EC2::CustomerGateway
	Internet 网关	AWS::EC2::InternetGateway
	网络访问控制列表 (ACL)	AWS::EC2::NetworkAcl
	路由表	AWS::EC2::RouteTable
	子网	AWS::EC2::Subnet
	Virtual Private Cloud (VPC)	AWS::EC2::VPC
	VPN 连接	AWS::EC2::VPNConnection
	VPN 网关	AWS::EC2::VPNGateway

AWS 服务	资源类型	资源类型值
AWS WAF ⁹	基于速率的规则	AWS::WAF::RateBasedRule
	规则	AWS::WAF::Rule
	Web ACL	AWS::WAF::WebACL
	规则组	AWS::WAF::RuleGroup
	基于速率的规则	AWS::WAFRegional::RateBasedRule
	规则	AWS::WAFRegional::Rule
	Web ACL	AWS::WAFRegional::WebACL
	规则组	AWS::WAFRegional::RuleGroup

备注

1. AWS Config 会记录对 CloudFormation 堆栈和堆栈中支持的资源类型所做的配置更改。AWS Config 不会记录对堆栈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显示在堆栈的配置项的补充配置部分中。
2. 对 Amazon CloudFront 的 AWS Config 支持仅在美国东部 (弗吉尼亚北部) 区域提供。
3. 要了解有关 AWS Config 如何与 AWS CodeBuild 集成的更多信息，请参阅[将 AWS Config 与 AWS CodeBuild 示例配合使用](#)。
4. AWS 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 AWS 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 Amazon EC2 用户指南（适用于 Linux 实例）中的[使用 AWS Config 跟踪配置变更](#)。
5. 要了解有关托管实例清单的更多信息，请参阅[记录托管实例的软件配置 \(p. 8\)](#)。
6. AWS Identity and Access Management (IAM) 资源是全球性资源。全球性资源不限于某个区域，而是可以用于所有区域。全球性资源的配置详细信息在所有区域都相同。有关更多信息，请参阅[选择 AWS Config 所记录的资源 \(p. 124\)](#)。
7. AWS Config 包含的内联策略具有其记录的配置详细信息。
8. 如果您已将 AWS Config 配置为记录您的 S3 存储桶且不接收配置更改通知，请验证您的 S3 存储桶策略是否拥有所需权限。有关更多信息，请参阅[有关记录 S3 存储桶的疑难解答 \(p. 130\)](#)。
9. AWS WAF 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 AWS WAF 的区域提供。

记录托管实例的软件配置

您可以使用 AWS Config 记录 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，AWS 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 AWS 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 AWS Config 中打开对托管实例清单资源类型的记录
- 将 EC2 和本地实例配置为托管实例

- 启动收集托管实例的软件清单

您也使用 AWS 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，AWS Config 会将这个实例标记为违反了您的规则。有关 AWS Config 托管规则的列表，请参阅[AWS 托管配置规则 \(p. 28\)](#)。

在 AWS Config 中启用软件配置变更的记录：

1. 在 AWS 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 AWS Config 所记录的资源 \(p. 124\)](#)。
2. 启动具有 IAM 角色和 AmazonEC2RoleforSSM 策略的 Amazon EC2 实例。您可能还需要安装 [SSM 代理](#)。有关更多信息，请参阅 [Systems Manager 先决条件](#) 在 Amazon EC2 用户指南（适用于 Linux 实例）中，或 Amazon EC2 用户指南（适用于 Windows 实例）中的 [Systems Manager 先决条件](#)。
3. 启动清单收集，详情请参考 Amazon EC2 用户指南（适用于 Linux 实例）中的 [配置清单收集](#)。Linux 和 Windows 实例的步骤相同。

AWS Config 可以记录以下清单类型的配置变更：

- Applications – 托管实例的应用程序列表，例如杀毒软件。
- AWS components – 托管实例的 AWS 组件列表，例如 AWS CLI 和软件开发工具包。
- Instance information – 实例信息，例如操作系统名称和版本、域，以及防火墙状态。
- Network configuration – 配置信息，例如 IP 地址、网关和子网掩码。
- Windows Updates – 托管实例的 Windows 更新列表（仅适用于 Windows 实例）。

Note

AWS Config 目前不支持记录自定义清单类型。

除了收集清单，Amazon EC2 Systems Manager 还有许多功能，其中包括应用操作系统补丁，和大规模配置实例。有关更多信息，请参阅 [Amazon EC2 Systems Manager](#) 在 Amazon EC2 用户指南（适用于 Linux 实例）中，或 Amazon EC2 用户指南（适用于 Windows 实例）中的 [Amazon EC2 Systems Manager](#)。

配置项的组成部分

配置项由以下部分组成。

组件	描述	包含
元数据	有关此配置项的信息	<ul style="list-style-type: none"> • 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 ¹	资源属性	<ul style="list-style-type: none"> • 资源 ID • 此资源的键-值标签列表³ • 资源类型；请参阅支持的 AWS 资源类型 (p. 6) • Amazon 资源名称 (ARN) • 包含此资源的可用区（如果适用） • 资源创建的时间

组件	描述	包含
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	<p>例如，DescribeVolumes API 会返回有关卷的以下信息：</p> <ul style="list-style-type: none"> 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 DeleteOnTermination 标记的状态 卷挂载到的设备 卷类型，例如 gp2, io1, 或 standard

备注

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. AWS Config 还会记录 Amazon S3 存储桶资源类型的以下属性。有关这些属性的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的[存储桶配置选项](#)。
3. AWS Config 不记录 CloudTrail 跟踪、CloudFront 分配和 CloudFront 串流分配的键-值标签。
4. 从 1.3 版开始，relatedEvents 字段为空。您可以访问 AWS CloudTrail API Reference 中的 [LookupEvents API](#) 来检索资源的事件。
5. 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。

Amazon S3 存储桶属性

属性	说明
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 AWS 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。

属性	说明
VersioningConfiguration	对存储桶中的对象启用版本控制。

支持的资源关系

AWS Config 支持不同资源之间存在以下关系。

Note

变更资源并且该资源与其他资源关联时，AWS Config 会创建多个配置项。有关更多信息，请参阅[存在关系的资源的配置项 \(p. 95\)](#)。

资源	关系	相关资源
Auto Scaling 组	包含	Amazon EC2 实例
	关联到	传统负载均衡器
		Auto Scaling 启动配置
		子网
Auto Scaling 启动配置	关联到	Amazon EC2 安全组
Auto Scaling 扩展策略	关联到	Auto Scaling 组
		警报
Auto Scaling 计划操作	关联到	Auto Scaling 组
Amazon EBS 卷	挂载到	EC2 实例
Amazon Redshift 群集	关联到	群集参数组
		群集安全组
		群集子网组
		安全组
		Virtual Private Cloud (VPC)
Amazon Redshift 群集快照	关联到	集群
		Virtual Private Cloud (VPC)
Amazon Redshift 群集子网组	关联到	子网
		Virtual Private Cloud (VPC)
AWS CloudFormation 堆栈	包含	支持的 AWS 资源类型
Amazon CloudFront 分配	关联到	AWS WAF WebACL
		ACM 证书
		S3Bucket
		IAM 服务器证书

资源	关系	相关资源
Amazon CloudFront 流分配	关联到	AWS WAF WebACL
		ACM 证书
		S3Bucket
		IAM 服务器证书
AWS CodeBuild 项目	关联到	S3Bucket
		IAM 角色
客户网关	挂载到	VPN 连接
EC2 专用主机	包含	EC2 实例
EC2 弹性 IP (EIP)	挂载到	EC2 实例
		网络接口
EC2 实例	包含	EC2 网络接口
	关联到	EC2 安全组
	挂载到	Amazon EBS 卷
		EC2 弹性 IP (EIP)
	包含在	EC2 专用主机
		路由表
		子网
		Virtual Private Cloud (VPC)
EC2 托管实例清单	关联到	EC2 实例
EC2 网络接口	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)
EC2 安全组	关联到	EC2 实例
		EC2 网络接口
		Virtual Private Cloud (VPC)
Elastic Load Balancing 应用程序负载均衡器	关联到	EC2 安全组
	挂载到	子网
	包含在	Virtual Private Cloud (VPC)

资源	关系	相关资源
Elastic Load Balancing Classic 负载均衡器	关联到	EC2 安全组
	挂载到	子网
	包含在	Virtual Private Cloud (VPC)
IAM 客户管理的政策	挂载到	IAM 用户
		IAM 组
		IAM 角色
IAM 组	包含	IAM 用户
	挂载到	IAM 客户管理的政策
IAM 角色	挂载到	IAM 客户管理的政策
IAM 用户	挂载到	IAM 组
		IAM 客户管理的政策
Internet 网关	挂载到	Virtual Private Cloud (VPC)
网络 ACL	挂载到	子网
	包含在	Virtual Private Cloud (VPC)
RDS 数据库实例	关联到	EC2 安全组
		RDS 数据库安全组
		RDS 数据库子网组
RDS 数据库安全组	关联到	EC2 安全组
		Virtual Private Cloud (VPC)
RDS 数据库快照	关联到	Virtual Private Cloud (VPC)
RDS 数据库子网组	关联到	EC2 子网
		Virtual Private Cloud (VPC)
路由表	包含	EC2 实例
		EC2 网络接口
		子网
		VPN 网关
	包含在	Virtual Private Cloud (VPC)
子网	包含	EC2 实例
		EC2 网络接口
	挂载到	网络 ACL
	包含在	路由表

资源	关系	相关资源
		Virtual Private Cloud (VPC)
Virtual Private Cloud (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
		VPN 网关
VPN 连接	挂载到	客户网关
		VPN 网关
VPN 网关	挂载到	Virtual Private Cloud (VPC)
		VPN 连接
	包含在	路由表
WAF WebACL	关联到	WAF 规则
		WAF 基于速率的规则
		WAF RuleGroup
WAFRegional WebACL	关联到	ElasticLoadBalancingV2 LoadBalancer
		WAFRegional 规则
		WAFRegional 基于速率的规则
		WAFRegional RuleGroup
WAF RuleGroup	关联到	WAF 规则
WAF 区域 RuleGroup	关联到	WAFRegional 规则

AWS Config 入门

在您注册 AWS 账户之后，您可以使用 AWS 管理控制台、AWS CLI 或 AWS 开发工具包开始使用 AWS Config。使用控制台可以加快和简化流程。

在您设置 AWS Config 时，可以完成以下操作：

- 指定您希望 AWS 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。
- 授予 AWS Config 所需的权限，用于访问 Amazon S3 存储桶与 SNS 主题。
- 指定您希望 AWS 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 AWS CLI 的更多信息，请参阅[使用 AWS CLI 设置 AWS Config \(p. 19\)](#)。

有关如何使用 AWS SDKs 的更多信息，请参阅[适用于 AWS Config 的 AWS 开发工具包 \(p. 147\)](#)。

主题

- [注册 AWS \(p. 15\)](#)
- [使用控制台设置 AWS Config \(p. 15\)](#)
- [使用 AWS CLI 设置 AWS Config \(p. 19\)](#)
- [查看 AWS Config 控制面板 \(p. 24\)](#)

注册 AWS

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

如果您没有 AWS 账户，请通过以下步骤创建一个账户。

注册 AWS

1. 打开 <https://aws.amazon.com/>，然后选择 Create an AWS Account。
2. 按照屏幕上的说明进行操作。

使用控制台设置 AWS Config

您可以通过 AWS 管理控制台来开始使用 AWS Config 执行以下操作：

- 指定您希望 AWS Config 记录的资源类型。
- 设置 Amazon SNS 以通知您配置更改。
- 指定 Amazon S3 存储桶以接收配置信息。
- 添加 AWS Config 托管规则以评估资源类型。

如果您是首次使用 AWS Config 或者为新区域配置 AWS Config，您可以选择托管规则来评估资源配置。有关支持 AWS Config 和 AWS Config 规则的区域，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。

使用控制台设置 AWS Config

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 如果这是您首次打开 AWS Config 控制台或者您在新区域中设置 AWS Config，AWS Config 控制台页面与以下类似：



3. 选择 Get Started Now。
4. 在 Settings 页面上，对于 Resource types to record，请指定您希望 AWS Config 记录的 AWS 资源类型：
 - All resources – AWS Config 会使用下列选项记录所有受支持的资源：
 - Record all resources supported in this region – AWS Config 将记录区域性资源的每种受支持类型的配置更改。在 AWS Config 添加对新资源类型的支持后，AWS Config 将自动开始记录该类型的资源。
 - Include global resources – AWS Config 将受支持类型的全局性资源包括在它所记录的资源（例如 IAM 资源）中。在 AWS Config 添加对新全球性资源类型的支持后，AWS Config 将自动开始记录该类型的资源。
 - Specific types – AWS Config 仅记录您指定的 AWS 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 AWS Config 所记录的资源 \(p. 124\)](#)。

5. 对于 Amazon S3 存储桶，选择 AWS Config 将配置历史记录和配置快照文件发送到的 Amazon S3 存储桶：
 - 创建新的存储桶 – 对于 存储桶名称，请键入您的 Amazon S3 存储桶的名称。

您键入的名称在 Amazon S3 现有的所有存储桶名称中必须具有唯一性。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 开发人员指南 中的 [存储桶局限和限制](#)。
 - Choose a bucket from your account – 对于 存储桶名称，请选择您的首选存储桶。

- 从另一个账户选择一个存储桶 – 对于存储桶名称，请键入存储桶名称。

如果您从其他账户选择存储桶，则该存储桶必须拥有授予 AWS Config 访问权限的策略。有关更多信息，请参阅 [针对 Amazon S3 存储桶的权限 \(p. 130\)](#)。

6. 对于 Amazon SNS Topic，通过选择 Stream configuration changes and notifications to an Amazon SNS topic 来选择 AWS Config 是否对信息进行流式处理。AWS Config 发送配置历史记录传输、配置快照传输和合规性等通知。
7. 如果您选择让 AWS Config 将信息流式传输到 Amazon SNS 主题，请选择目标主题：
 - 创建一个新主题 – 对于 主题名称，请键入您的 SNS 主题的名称。
 - 从您的账户选择一个主题 – 对于 主题名称，请选择您的首选主题。
 - 从另一个账户选择一个主题 – 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 AWS Config 访问权限的策略。有关更多信息，请参阅 [Amazon SNS 主题的权限 \(p. 132\)](#)。

Note

Amazon SNS 主题所在的区域必须与您设置 AWS Config 的区域相同。

8. 对于 AWS Config role，选择一个 IAM 角色，以授予 AWS Config 记录配置信息并将此信息发送到 Amazon S3 和 Amazon SNS 的权限：
 - Create a role – AWS Config 创建具备所需权限的角色。对于 Role name，您可以自定义 AWS Config 创建的角色的名称。
 - Choose a role from your account – 对于 Role name，从您的账户中选择一个 IAM 角色。AWS Config 将附加所需的策略。有关更多信息，请参阅 [分配给 AWS Config 的 IAM 角色权限 \(p. 128\)](#)。

Note

如果您希望按原样使用 IAM 角色，请选中该框。AWS Config 不会将策略附加到角色。

9. 如果您在支持规则的区域中设置 AWS Config，请选择 Next。请参阅 [使用控制台设置 AWS Config \(p. 17\)](#)。

否则，请选择 Save。AWS Config 将显示 Resource inventory 页面。

有关查找账户中现有资源及了解资源配置的信息，请参阅 [View, and Manage Your AWS Resources \(p. 78\)](#)。

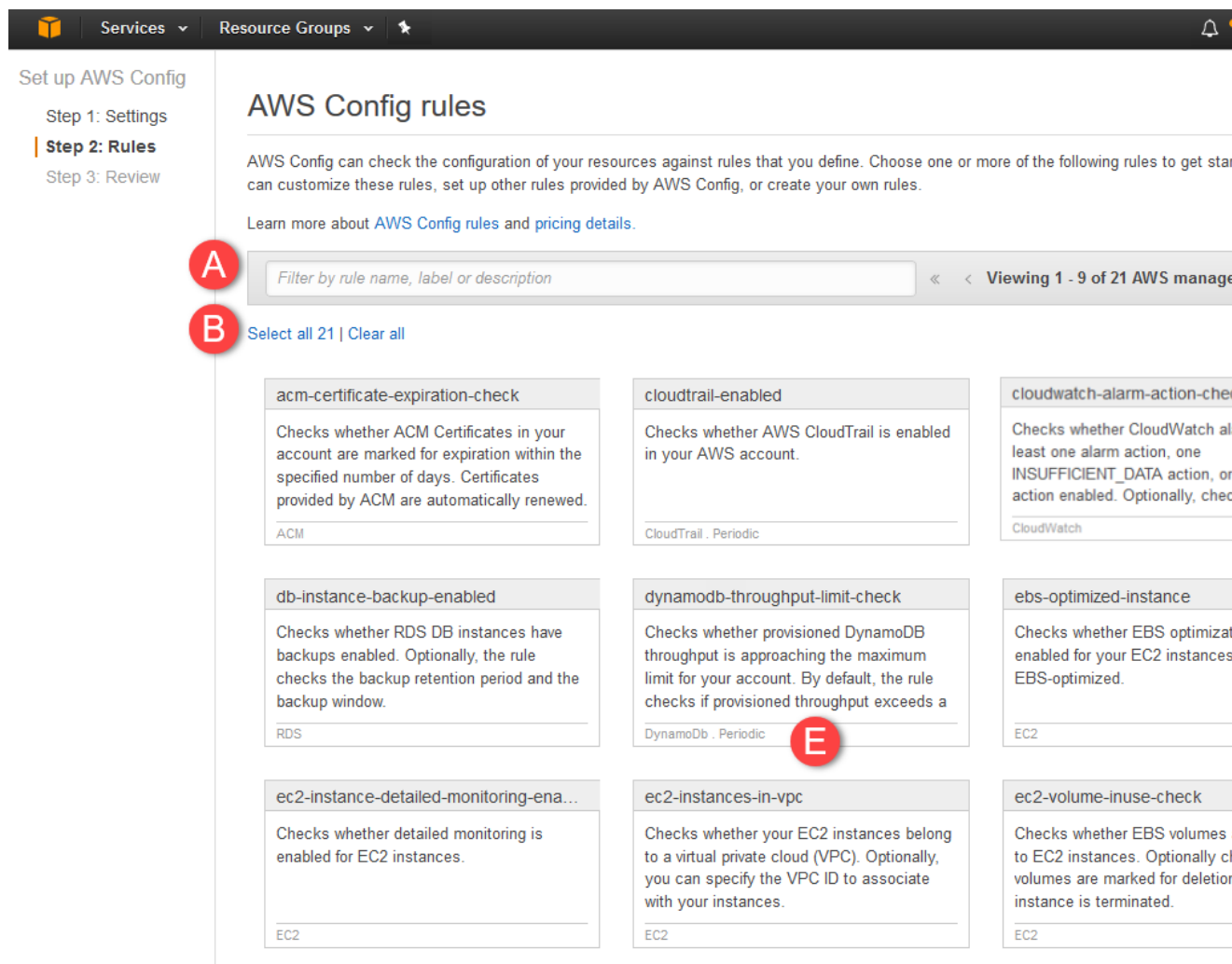
如果您选择让 AWS Config 将信息流式传输到 Amazon SNS 主题，则可以通过电子邮件接收通知。有关更多信息，请参阅 [通过电子邮件监控 AWS Config 资源变更 \(p. 90\)](#)。您也可以使用 Amazon Simple Queue Service 以编程方式来监控 AWS 资源。有关更多信息，请参阅 [使用 Amazon SQS 监控 AWS 资源更改 \(p. 136\)](#)。

使用控制台设置 AWS Config

Rules 页面提供了初始 AWS 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，AWS Config 根据您的选择的规则来评估您的 AWS 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 AWS 托管规则的完整列表，请参阅 [AWS 托管配置规则 \(p. 28\)](#)。

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，AWS 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：

- A. 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 [AWS Config 规则指定触发器 \(p. 26\)](#)。
- B. 选择 Select all 以添加所有规则，或者选择 Clear all 以删除所有规则。
- C. 选择箭头图标可查看下一页规则。
- D. 最近添加的规则标记为 New。
- E. 查看标签来确定规则所评估的服务以及规则是否具有定期触发器。

设置 AWS 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。
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 AWS Config 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...。您可以使用刷新按钮更新结果。当 AWS 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 \(p. 69\)](#)。

Note

AWS Config 仅评估它所记录的资源类型。例如，如果您添加 cloudtrail-enabled 规则但未记录 CloudTrail 跟踪资源类型，AWS Config 无法评估您账户中的跟踪是否合规。有关更多信息，请参阅 [选择 AWS Config 所记录的资源 \(p. 124\)](#)。

您可以查看、编辑和删除现有规则。您还可以创建额外的 AWS 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 AWS Config 规则 \(p. 72\)](#)。

使用 AWS CLI 设置 AWS Config

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

有关 AWS CLI 的更多信息以及 AWS CLI 工具的安装说明，请参阅 AWS Command Line Interface 用户指南中的以下内容。

- [AWS Command Line Interface 用户指南](#)
- [开始设置 AWS Command Line Interface](#)

请参阅以下主题，以使用 AWS CLI 设置 AWS Config。当您设置 AWS 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 AWS Config 设置规则的更多信息，请参阅 [使用 AWS CLI \(p. 74\)](#)。

主题

- [先决条件 \(p. 19\)](#)
- [启用 AWS Config \(p. 22\)](#)
- [验证 AWS Config 是否打开 \(p. 22\)](#)

先决条件

按照此过程，使用附加的策略创建 Amazon S3 存储桶、Amazon SNS 主题和 IAM 角色。然后，您可以使用 AWS CLI 为 AWS Config 指定存储桶、主题和角色。

内容

- [创建 Amazon S3 存储段 \(p. 19\)](#)
- [创建 Amazon SNS 主题 \(p. 20\)](#)
- [创建 IAM 角色 \(p. 21\)](#)

创建 Amazon S3 存储段

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 \(p. 20\)](#)。

要使用 AWS CLI 创建 Amazon S3 存储桶，请使用 `create-bucket` 命令。

使用控制台创建 Amazon S3 存储桶

1. 登录 AWS 管理控制台并通过以下网址打开 Amazon S3 控制台：<https://console.aws.amazon.com/s3/>。

2. 选择 Actions，然后选择 Delete Bucket。
3. 对于 Bucket Name:，请键入您的 Amazon S3 存储桶的名称，例如 *my-config-bucket*。

Note

请确保您选择的存储桶名称在所有现有 Amazon S3 存储桶名称中是唯一名称。存储桶创建完毕后，您将无法更改其名称。有关存储桶命名规则和约定的更多信息，请参阅 [Amazon Simple Storage Service 开发人员指南](#) 中的存储桶限制。

4. 选择 Create。

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 AWS Config 授予访问权限。有关授予 Amazon S3 存储桶访问权限的信息，请参阅 [针对 Amazon S3 存储桶的权限 \(p. 130\)](#)，然后转至 [创建 Amazon SNS 主题 \(p. 20\)](#)。

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 \(p. 21\)](#)。

要使用 AWS CLI 创建 Amazon SNS 主题，请使用 [create-topic](#) 命令。

使用控制台创建 Amazon SNS 主题

1. 通过以下网址登录 AWS 管理控制台 并打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v2/home>。
2. 选择 Create New Topic。
3. 对于 Topic Name，请为键入您的 SNS 主题的名称，例如 *my-config-notice*。
4. 选择 Create Topic。

新建主题在“Topic Details”页面显示。为下一个任务复制“Topic ARN”。

有关更多信息，请参阅 AWS General Reference 中的 [ARN 格式](#)。

要接收 AWS Config 通知，您必须使用电子邮件地址订阅主题。

使用电子邮件地址订阅 SNS 主题

1. 在 Amazon SNS 控制台中，选择导航窗格中的 Subscriptions。
2. 在 Subscriptions 页面，选择 Create Subscription。
3. 对于 Topic ARN，请粘贴您在上一任务中复制的主题 ARN。
4. 对于 Protocol，选择 Email。
5. 对于 Endpoint，键入您用于接收通知的电子邮件地址，然后选择 Subscribe。
6. 进入您的电子邮件应用程序，然后打开来自 AWS Notifications 的消息。选择链接确认您的订阅。

您的 Web 浏览器将显示来自 Amazon SNS 的确认响应。Amazon SNS 现已配置为以电子邮件形式接收通知并将通知发送到指定的电子邮件地址。

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授予 AWS Config 访问权限。有关授予 Amazon SNS 主题访问权限的信息，请参阅 [Amazon SNS 主题的权限 \(p. 132\)](#)，然后转至 [创建 IAM 角色 \(p. 21\)](#)。

创建 IAM 角色

您可使用 IAM 控制台来创建 IAM 角色以便授予 AWS Config 权限，使其可以访问您的 Amazon S3 存储桶、访问您的 Amazon SNS 主题，并获取受支持的 AWS 资源的配置详细信息。创建 IAM 角色后，您需要创建策略并将其关联到该角色。

要使用 AWS CLI 创建 IAM 角色，请使用 `create-role` 命令。然后，您可以使用 `attach-role-policy` 命令将策略附加到角色。

使用控制台创建 IAM 角色

1. 登录 AWS 管理控制台 并通过以下网址打开 IAM 控制台 <https://console.aws.amazon.com/iam/>。
2. 在 IAM 控制台中，选择导航窗格中的 Roles，然后选择 Create New Role。
3. 对于 Role Name，请键入可描述此角色作用的名称。角色名称在您的 AWS 账户内必须是唯一的。由于可能有多种实体引用该角色，在您创建角色后不能编辑角色名称。

选择 Next Step。

4. 选择 AWS Service Roles，然后为 AWS Config 选择 Select。
5. 在 Attach Policy 页面，选择 AWSConfigRole。这一 AWS 托管策略可以授予 AWS Config 权限，使其可以获取受支持的 AWS 资源的配置详细信息，然后选择 Next Step。
6. 在 Review 页面，查看您的角色的详细信息，然后选择 Create Role。
7. 在 Roles 页面，选择您创建的角色以便打开其详细信息页面。

您可以创建允许 AWS Config 访问您的 Amazon S3 存储桶与 Amazon SNS 主题的内联策略，从而扩大角色权限。

创建授权 AWS Config 访问您的 Amazon S3 存储桶的内联策略

1. 在 Permissions 部分中，展开 Inline Policies 部分，然后选择 click here。
2. 选择 Custom Policy，然后选择 Select。
3. 对于 Policy Name，请键入您的内联策略名称。
4. 复制 [用于 Amazon S3 存储桶的 IAM 角色策略 \(p. 129\)](#) 中的示例 Amazon S3 存储桶策略，然后将其粘贴到 Policy Document 编辑器中。

Important

在您继续下一步之前，请替换策略中的以下值。如果不替换这些值，您的策略就不会发挥作用。

- `myBucketName` – 替换为您的 Amazon S3 存储桶名称。
- `prefix` – 替换为您自己的前缀，或删除后面的 `/` 以留空。
- `myAccountID-WithoutHyphens` – 替换为您的 AWS 帐户 ID。

5. 选择 Apply Policy。

创建授权 AWS Config 向您的 Amazon SNS 主题发送通知的内联策略

1. 在 Permissions 部分中，展开 Inline Policies 部分，然后选择 click here。
2. 选择 Custom Policy，然后选择 Select。
3. 对于 Policy Name，请键入您的内联策略名称。
4. 复制 [用于 Amazon SNS 主题的内联策略 \(p. 129\)](#) 中的 Amazon SNS 主题示例策略，然后将其粘贴到 Policy Document 编辑器中。

Important

在您继续下一步之前，请使用您在创建 Amazon SNS 主题时保存的 ARN 替换
`arn:aws:sns:region:account-id:myTopic`。

5. 选择 Apply Policy。

启用 AWS Config

您可以在 AWS CLI 中使用 `subscribe` 命令和若干参数来启用 AWS Config。

您可以使用 `subscribe` 命令，以让 AWS Config 开始记录您账户中支持的所有 AWS 资源的配置。该 `subscribe` 命令会创建一个配置记录器以及一条使用指定 Amazon S3 存储桶和 Amazon SNS 主题的传递通道，并开始记录相关配置项。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。

要启用 AWS Config，请使用 `subscribe` 及以下参数：

`subscribe` 命令使用以下选项：

`--s3-bucket`

指定您的账户或其他账户中现有的某个 Amazon S3 存储桶的名称。

`--sns-topic`

指定您的账户或其他账户中现有的某个 SNS 主题的 Amazon 资源名称 (ARN)。

`--iam-role`

指定某个现有 IAM 角色的 Amazon 资源名称 (ARN)。

指定的 IAM 角色必须关联有相关策略，以便授予 AWS Config 向 Amazon S3 存储桶和 Amazon SNS 主题传递配置项的权限，并且该角色还必须向支持的 AWS 资源的 Describe API 授予相关权限。

您的命令应类似于以下示例：

```
$ aws configservice subscribe --s3-bucket my-config-bucket --sns-topic arn:aws:sns:us-east-2:012345678912:my-config-notice --iam-role arn:aws:iam::012345678912:role/myConfigRole
```

在您运行 `subscribe` 命令之后，AWS Config 会记录它在该区域中找到的所有支持资源。如果您不希望 AWS Config 记录支持的资源，则可以通过更新配置记录器以使用记录组来指定要记录的资源类型。有关更多信息，请参阅 [选择资源 \(AWS CLI\)](#) (p. 125)。

验证 AWS Config 是否打开

打开 AWS Config 后，您便可使用 AWS CLI 命令验证 AWS Config 是否正在运行以及 `subscribe` 命令是否创建了配置记录器和传递通道。您也可以确认 AWS Config 是否已开始记录配置并向传递通道传递这些配置。

内容

- [验证是否已创建传递通道](#) (p. 22)
- [验证是否已创建配置记录器](#) (p. 23)
- [验证 AWS Config 是否已开始记录](#) (p. 23)

验证是否已创建传递通道

使用 `describe-delivery-channels` 命令验证是否已配置 Amazon S3 存储桶和 Amazon SNS 主题。

```
$ 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 SDK 来配置传递通道，且不指定名称时，AWS Config 会自动分配“default”这一名称。

验证是否已创建配置记录器

使用 `describe-configuration-recorders` 命令验证是否已创建配置记录器以及该配置记录器是否担任了 IAM 角色。有关更多信息，请参阅 [创建 IAM 角色 \(p. 21\)](#)。

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

验证 AWS Config 是否已开始记录

使用 `describe-configuration-recorder-status` 命令验证 AWS Config 是否已开始记录您账户中现有受支持的 AWS 资源的配置。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。AWS Config 采用 UTC 格式 (GMT - 8:00) 来记录时间。

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 [View, and Manage Your AWS Resources \(p. 78\)](#)。

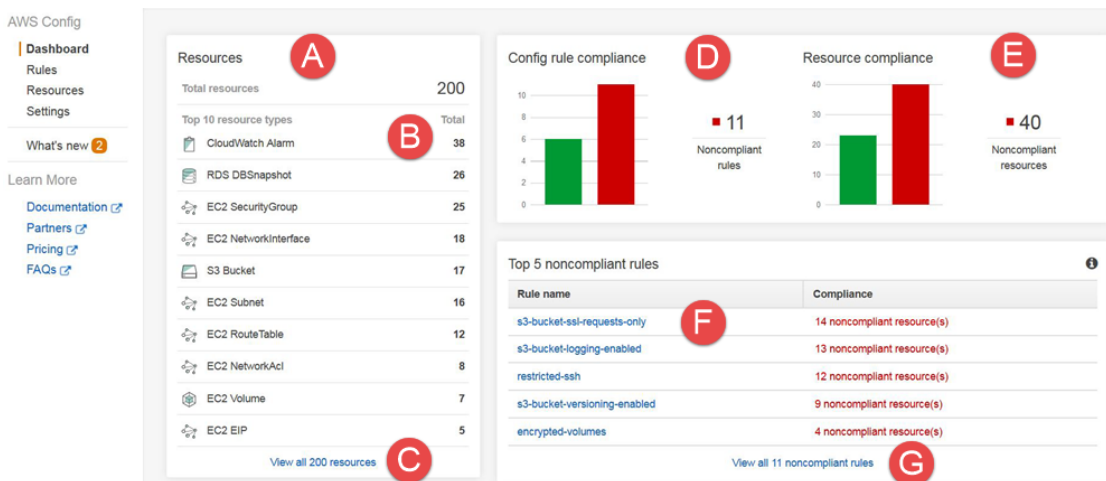
查看 AWS Config 控制面板

使用 Dashboard 可查看您的资源、规则及其合规性状态的概览。此页面可帮助您快速识别账户中的前几个资源，以及是否有任何不合规的规则或资源。

安装后，AWS Config 会开始记录指定的资源，然后根据您的规则对其进行评估。AWS Config 可能需要几分钟时间在 Dashboard 上显示您的资源、规则及其合规性状态。

使用 AWS Config 控制面板

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 选择 Dashboard。
3. 使用 Dashboard 可查看您的资源、规则及其合规性状态的概览。



在 Dashboard 上，可以执行以下操作：

- A. 查看 AWS Config 正在记录的资源的总数。
- B. 以降序顺序查看 AWS Config 正在记录的资源类型 (资源的数量)。选择一个资源类型以转至 Resources inventory 页面。
- C. 选择 View all resources 以转至 Resources inventory 页面。
- D. 查看不合规规则的数量。
- E. 查看不合规资源的数量。
- F. 以降序顺序查看前几条不合规规则 (资源的数量)。
- G. 选择 View all noncompliant rules 以转至 Rules 页面。

Dashboard 显示特定于您的区域和账户的资源 and 规则。它不会显示其他区域或其他 AWS 账户中的资源或规则。

Note

Evaluate your AWS resource configuration using Config rules 消息可能会出于以下原因显示在 Dashboard 上：

- 您尚未为您的账户设置 AWS Config 规则。您可以选择 Add rule 以转到 Rules 页面。
- AWS 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。

- AWS 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 Settings 页面中指定 AWS Config 要记录的资源。有关更多信息，请参阅 [选择 AWS Config 所记录的资源 \(p. 124\)](#)。

使用 AWS Config 规则评估资源

使用 AWS Config 评估您的 AWS 资源的配置设置。您可以通过创建 AWS Config 规则进行评估，规则规定了您理想的配置设置。AWS Config 能够提供可自定义的预定义规则 (称作托管规则)，以帮助您开始进行评估。您还可以创建自己的自定义规则。在 AWS 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，那么 AWS Config 会将该资源和规则标记为不合规。

例如，当创建 EC2 卷时，AWS 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，AWS Config 会将卷和规则标记为不合规。AWS 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，AWS Config 可以检查账户中 EC2 卷的数量是否在所需总数以内，或者账户是否使用 AWS CloudTrail 进行登录。

AWS 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 AWS 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 AWS CLI、AWS Config API 和 AWS 软件开发工具包请求 AWS Config 服务，以获取合规性信息。

通过使用 AWS 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。

有关支持 AWS Config 规则的区域的信息，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。

您在自己的账户中对每个区域最多可创建 50 条 AWS Config 规则。有关更多信息，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 限制](#)。

您还可以创建自定义规则来评估 AWS 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 \(p. 61\)](#)。

主题

- [为 AWS Config 规则指定触发器 \(p. 26\)](#)
- [关于 AWS 托管 Config 规则 \(p. 28\)](#)
- [为 AWS Config 制定自定义规则 \(p. 56\)](#)
- [查看配置合规性 \(p. 69\)](#)
- [管理您的 AWS Config 规则 \(p. 72\)](#)
- [手动评估您的资源 \(p. 76\)](#)

为 AWS 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 AWS Config 何时运行此规则；这称作触发器。当触发器触发时，AWS Config 对照规则对您的资源配置进行评估。

内容

- [触发器类型 \(p. 26\)](#)
- [具有触发器的规则示例 \(p. 27\)](#)
- [关闭配置记录器时的规则评估 \(p. 27\)](#)

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，AWS 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

AWS 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

AWS Config 按照您选择的频率运行规则的评估（例如，每 24 小时）。

如果您选择进行配置更改和定期，AWS Config 会在检测到配置更改时调用您的 Lambda 函数，并按照您指定的频率进行。

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. 通过向账户中添加 AWS Config 托管规则 `S3_BUCKET_LOGGING_ENABLED` 来检查您的 Amazon S3 存储桶是否启用了日志记录。
2. 此规则的触发器类型为配置更改。在创建、更改或删除 Amazon S3 存储桶时，AWS Config 运行规则评估。
3. 当存储桶更新时，配置更改触发此规则，AWS 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. 向账户中添加 AWS 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。AWS Config 以您指定的频率（如每 24 小时）运行规则评估。
3. 此规则每 24 小时触发一次，并由 AWS 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自己的账户是否启用了 CloudTrail 跟踪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 AWS Config 都运行规则评估。您还希望 AWS 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，AWS 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。

- 如果您为具有配置更改触发器的规则运行按需评估，规则将评估资源的最后已知状态，这是最后记录的配置项目。有关按需评估的更多信息，请参阅[手动评估您的资源 \(p. 76\)](#)。

关于 AWS 托管 Config 规则

AWS Config 能够提供可自定义的预定义 AWS 托管规则，并使用这些规则来评估您的 AWS 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快速开始评估您的 Amazon Elastic Block Store (Amazon EBS) 卷是否已加密，或者特定标签是否已应用到您的资源。您可以设置和激活这些规则而无需通过编写代码来创建 AWS Lambda 函数，如果您想要创建自定义规则这就是必需的。AWS 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 AWS Command Line Interface 或 AWS Config API 来传递用于定义您的托管规则配置的 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，AWS 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，AWS 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：

- 配置更改触发 – 当与规则范围匹配的任何资源的配置更改时，AWS Config 将触发评估。在 AWS Config 发送配置项更改通知后，评估便会运行。
- Periodic – AWS Config 按照您选择的频率运行评估（例如，每 24 小时）。

AWS 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 \(p. 69\)](#)。

主题

- [AWS 托管配置规则 \(p. 28\)](#)
- [使用 AWS 托管规则 \(p. 55\)](#)
- [使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)

AWS 托管配置规则

AWS Config 提供以下托管规则。

计算

- [approved-amis-by-id \(p. 30\)](#)
- [approved-amis-by-tag \(p. 31\)](#)
- [autoscaling-group-elb-healthcheck-required \(p. 31\)](#)
- [desired-instance-tenancy \(p. 36\)](#)
- [desired-instance-type \(p. 37\)](#)
- [ebs-optimized-instance \(p. 39\)](#)
- [ec2-instance-detailed-monitoring-enabled \(p. 39\)](#)
- [ec2-instances-in-vpc \(p. 39\)](#)
- [ec2-managedinstance-applications-blacklisted \(p. 40\)](#)
- [ec2-managedinstance-applications-required \(p. 40\)](#)
- [ec2-managedinstance-inventory-blacklisted \(p. 41\)](#)
- [ec2-managedinstance-platform-check \(p. 41\)](#)
- [ec2-volume-inuse-check \(p. 42\)](#)

- [eip-attached](#) (p. 42)
- [encrypted-volumes](#) (p. 44)
- [elb-acm-certificate-required](#) (p. 43)
- [elb-custom-security-policy-ssl-check](#) (p. 43)
- [elb-predefined-security-policy-ssl-check](#) (p. 44)
- [restricted-common-ports](#) (p. 51)
- [restricted-ssh](#) (p. 51)

Database

- [db-instance-backup-enabled](#) (p. 36)
- [dynamodb-autoscaling-enabled](#) (p. 37)
- [dynamodb-throughput-limit-check](#) (p. 38)
- [rds-multi-az-support](#) (p. 48)
- [rds-storage-encrypted](#) (p. 49)
- [redshift-cluster-configuration-check](#) (p. 49)
- [redshift-cluster-maintenancesettings-check](#) (p. 50)

管理工具

- [cloudtrail-enabled](#) (p. 32)
- [cloudformation-stack-notification-check](#) (p. 31)
- [cloudwatch-alarm-action-check](#) (p. 33)
- [cloudwatch-alarm-resource-check](#) (p. 34)
- [cloudwatch-alarm-settings-check](#) (p. 34)
- [codebuild-project-envvar-awscred-check](#) (p. 35)
- [codebuild-project-source-repo-url-check](#) (p. 35)
- [required-tags](#) (p. 50)

安全、身份和合规性

- [acm-certificate-expiration-check](#) (p. 30)
- [fms-webacl-resource-policy-check](#) (p. 45)
- [fms-webacl-rulegroup-association-check](#) (p. 45)
- [iam-group-has-users-check](#) (p. 47)
- [iam-password-policy](#) (p. 46)
- [iam-user-group-membership-check](#) (p. 47)
- [iam-user-no-policies-check](#) (p. 48)
- [root-account-mfa-enabled](#) (p. 52)

存储

- [s3-bucket-logging-enabled](#) (p. 52)
- [s3-bucket-public-read-prohibited](#) (p. 53)*
- [s3-bucket-public-write-prohibited](#) (p. 53)*
- [s3-bucket-server-side-encryption-enabled](#) (p. 53)*
- [s3-bucket-ssl-requests-only](#) (p. 54)*

- [s3-bucket-versioning-enabled](#) (p. 54)

* 此规则使用自动推理工具 (ART) 来评估 IAM 权限和资源策略的正确性。

acm-certificate-expiration-check

检查您账户中的 ACM 证书是否标记为将在指定天数内过期。将自动续订由 ACM 提供的证书。ACM 不会自动续订您导入的证书。

标识符：ACM_CERTIFICATE_EXPIRATION_CHECK

触发类型：配置更改和定期

参数：

daysToExpiration

指定规则将 ACM 证书标记为不合规之前的天数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则](#) (p. 56)。

查看	启动
查看	

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。具有此列表中未包含的 AMI 的运行实例不合规。

Identifier: APPROVED_AMIS_BY_ID

Trigger type: 配置更改

参数：

amilds

AMI ID (逗号分隔的列表，最多包含 10 个)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则](#) (p. 56)。

查看	启动
查看	

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。未包含至少一个指定标签的带 AMI 的运行实例不合规。

Identifier: APPROVED_AMIS_BY_TAG

Trigger type: 配置更改

参数:

amisByTagKeyAndValue

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”)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

autoscaling-group-elb-healthcheck-required

检查与负载均衡器关联的 Auto Scaling 组是否正在使用 Elastic Load Balancing 运行状况检查。

标识符: AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

cloudformation-stack-notification-check

检查您的 CloudFormation 堆栈是否正在向 SNS 主题发送事件通知。还可以检查是否使用了指定的 SNS 主题。

标识符: CLOUDFORMATION_STACK_NOTIFICATION_CHECK

Trigger type: 配置更改

参数:

snsTopic1

SNS 主题 ARN。

snsTopic2

SNS 主题 ARN。

snsTopic3

SNS 主题 ARN。

snsTopic4

SNS 主题 ARN。

snsTopic5

SNS 主题 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

cloudtrail-enabled

检查您的 AWS 账户中是否启用了 AWS CloudTrail。或者，您也可以指定要使用的 S3 存储桶、SNS 主题和 Amazon CloudWatch Logs ARN。

Identifier: CLOUD_TRAIL_ENABLED

Trigger type: 定期

参数:

s3BucketName

AWS CloudTrail 将日志文件传送到的 S3 存储桶的名称。

snsTopicArn

AWS CloudTrail 用于通知的 SNS 主题的 ARN。

cloudWatchLogsLogGroupArn

Amazon CloudWatch 将数据发送到的 AWS CloudTrail 日志组的 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

cloudwatch-alarm-action-check

检查 CloudWatch 警报是否至少启用了警报操作、一个 `INSUFFICIENT_DATA` 操作或一个 `OK` 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

Trigger type: 配置更改

参数:

`alarmActionRequired`

警报具有至少一个操作。

默认值为 `true`。

`insufficientDataActionRequired`

当警报从任意其他状态转换为 `INSUFFICIENT_DATA` 状态时，警报至少有一个操作。

默认值为 `true`。

`okActionRequired`

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。

默认值为 `false`。

`action1`

要执行的操作，指定为 ARN。

`action2`

要执行的操作，指定为 ARN。

`action3`

要执行的操作，指定为 ARN。

`action4`

要执行的操作，指定为 ARN。

`action5`

要执行的操作，指定为 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

cloudwatch-alarm-resource-check

检查指定的资源类型是否有针对指定指标的 CloudWatch 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_RESOURCE_CHECK

Trigger type: 定期

参数:

resourceType

AWS 资源类型。值可以是以下之一：

- AWS::EC2::Volume
- AWS::EC2::Instance
- AWS::S3::Bucket

metricName

与警报关联的指标的名称 (例如，对于 EC2 实例为“CPUUtilization”)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

cloudwatch-alarm-settings-check

检查拥有指定指标名称的 CloudWatch 警报是否具有指定设置。

标识符：CLOUDWATCH_ALARM_SETTINGS_CHECK

Trigger type: 配置更改

参数:

metricName

与警报关联的指标的名称。

threshold

指定统计数据的比较值。

evaluationPeriod

其中的数据将与指定阈值进行比较的期间数。

period

在其中应用指定统计数据的期间 (秒数)。

默认值为 300 秒。

comparisonOperator

比较指定的统计数据 and 阈值的操作 (例如, “GreaterThanThreshold”)。

统计数据

与警报关联的指标的统计数据 (例如, “平均值”或“总计”)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

codebuild-project-envvar-awscred-check

检查项目是否包含环境变量 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。如果项目环境变量中包含明文凭证, 则不符合此规则。

标识符: CODEBUILD_PROJECT_ENVVAR_AWSCRED_CHECK

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

codebuild-project-source-repo-url-check

检查 GitHub 或 Bitbucket 源存储库 URL 是否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 Bitbucket 存储库的行为兼容。

标识符: CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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。

Identifier: DB_INSTANCE_BACKUP_ENABLED

Trigger type: 配置更改

参数:

backupRetentionPeriod

备份的保留期。

preferredBackupWindow

创建备份的时间范围。

checkReadReplicas

检查 RDS 数据库实例是否已针对只读副本启用备份。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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。

Identifier: DESIRED_INSTANCE_TENANCY

Trigger type: 配置更改

参数:

租期

实例的期望租期。有效值包括 DEDICATED、HOST 和 DEFAULT。

imageId

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

Amazon EC2 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。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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 实例类型的列表，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[实例类型](#)。

Identifier: DESIRED_INSTANCE_TYPE

Trigger type: 配置更改

参数:

instanceType

逗号分隔的 EC2 实例类型列表 (例如“t2.small, m4.large, i2.xlarge”)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

dynamodb-autoscaling-enabled

此规则检查是否在 DynamoDB 表和/或全局辅助索引上启用了 Auto Scaling。(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

Trigger type: 定期

参数:

minProvisionedReadCapacity

应在 Auto Scaling 组中对读取容量配置的最小单位数。

minProvisionedWriteCapacity

应在 Auto Scaling 组中对写入容量配置的最小单位数。

maxProvisionedReadCapacity

应在 Auto Scaling 组中对读取容量配置的最大单位数。

maxProvisionedWriteCapacity

应在 Auto Scaling 组中对写入容量配置的最大单位数。

targetReadUtilization

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

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。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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%)。

Identifier: DYNAMODB_THROUGHPUT_LIMIT_CHECK

Trigger type: 定期

参数:

accountRCUThresholdPercentage

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，将规则标记为不合规。

accountWCUThresholdPercentage

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，将规则标记为不合规。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

ebs-optimized-instance

检查是否为可通过 EBS 优化的 EC2 实例启用 EBS 优化。

Identifier: EBS_OPTIMIZED_INSTANCE

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

ec2-instance-detailed-monitoring-enabled

检查是否已为 EC2 实例启用详细监控。

标识符 : EC2_INSTANCE_DETAILED_MONITORING_ENABLED

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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。

Identifier: INSTANCES_IN_VPC

Trigger type: 配置更改

参数:

vpclId

包含这些实例的 VPC 的 ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

ec2-managedinstance-applications-blacklisted

检查实例上未安装指定的任何应用程序。(可选) 指定应用程序版本。应用程序的较新版本不会被列入黑名单。您还可以指定平台，仅针对运行该平台的实例应用规则。

Identifier: EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

Trigger type: 配置更改

参数:

applicationNames

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”)。

注意：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-compatible**。此外，AWS Config 目前不支持对 applicationNames 参数使用通配符 (例如, **firefox***)。

platformType

平台类型 (例如, “Linux”或“Windows”)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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。

Identifier: EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

Trigger type: 配置更改

参数:

applicationNames

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”)。

注意: 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, AWS Config 目前不支持对 applicationNames 参数使用通配符 (例如, **firefox***)。

platformType

平台类型 (例如, “Linux”或“Windows”)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

ec2-managedinstance-inventory-blacklisted

检查由 AWS Systems Manager 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_BLACKLISTED

Trigger type: 配置更改

参数:

inventoryNames

以逗号分隔的 Systems Manager 清单类型列表 (例如“AWS:Network, AWS:WindowsUpdate”)。

platformType

平台类型 (例如, “Linux”)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

ec2-managedinstance-platform-check

检查 EC2 托管实例是否具有所需的配置。

Identifier: EC2_MANAGEDINSTANCE_PLATFORM_CHECK

Trigger type: 配置更改

参数:

agentVersion

代理版本 (例如, “2.0.433.0”)。

platformType

平台类型 (例如, “Linux”或“Windows”)。

platformVersion

平台版本 (例如, “2016.09”)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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

Trigger type: 配置更改

参数:

deleteOnTermination

EBS 卷已标记为在实例终止时删除。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

eip-attached

检查分配到某个 VPC 的所有弹性 IP 地址已连接到 EC2 实例, 还是正在使用的弹性网络接口 (ENI)。

评估发生后, 可能需要最多 6 小时才能获得结果。

Identifier: EIP_ATTACHED

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

elb-acm-certificate-required

检查传统负载均衡器是否使用 AWS Certificate Manager 提供的 SSL 证书。要使用此规则，请与传统负载均衡器配合使用 SSL 或 HTTPS 侦听器。此规则仅适用于传统负载均衡器。此规则不会检查应用程序负载均衡器和网络负载均衡器。

标识符 : ELB_ACM_CERTIFICATE_REQUIRED

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

elb-custom-security-policy-ssl-check

检查您的 传统负载均衡器 SSL 侦听器是否在使用自定义策略。此规则只适用于 传统负载均衡器 有 SSL 侦听器的情况。

标识符 : ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

Trigger type: 配置更改

参数:

ssl-protocols-and-ciphers

逗号分隔的密码和协议列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

elb-predefined-security-policy-ssl-check

检查您的 传统负载均衡器 SSL 侦听器是否在使用预定义策略。此规则只适用于 传统负载均衡器 有 SSL 侦听器的情况。

标识符：ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

Trigger type: 配置更改

参数:

predefined-policy-name

预定义策略的名称。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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。

有关更多信息，请参阅 Amazon EC2 用户指南（适用于 Linux 实例）中的[Amazon EBS 加密](#)。

Identifier: ENCRYPTED_VOLUMES

Trigger type: 配置更改

参数:

kmsId

用于加密卷的 KMS 密钥的 ID 或 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

fms-webacl-resource-policy-check

检查 Web ACL 是否与 应用程序负载均衡器 或 Amazon CloudFront 分配关联。当 AWS Firewall Manager 创建此规则时，FMS 策略所有者会在 FMS 策略中指定 `webACLId`，而且可以 (可选) 启用补救。

标识符：FMS_WEBACL_RESOURCE_POLICY_CHECK

Trigger type: 配置更改

参数:

`webACLId`

Web ACL 的 `WebACLId`。

`resourceTags`

规则应与之关联的资源标签 (应用程序负载均衡器 和 Amazon CloudFront 分配) (例如，`{ "tagKey1": ["tagValue1"], "tagKey2": ["tagValue2", "tagValue3"] }`)。

`excludeResourceTags`

如果为 `true`，则排除与 `resourceTags` 匹配的资源。

`fmsManagedToken`

在您的账户中创建规则时由 AWS Firewall Manager 生成的令牌。当您创建此规则时，AWS Config 会忽略此参数。

`fmsRemediationEnabled`

如果为 `true`，则 AWS Firewall Manager 将根据 FMS 策略更新不合规资源。当您创建此规则时，AWS Config 会忽略此参数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则](#) (p. 56)。

查看	启动
查看	

fms-webacl-rulegroup-association-check

检查 `RuleGroupId` 和 `WafOverrideAction` 对是否在最高优先级与 Web ACL 关联。当 AWS Firewall Manager 创建此规则时，FMS 策略所有者会在 FMS 策略中指定 `ruleGroups`，而且可以 (可选) 启用补救。

标识符：FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

Trigger type: 配置更改

参数:

ruleGroups

以逗号分隔的 RuleGroupIds 和 WafOverrideAction 对的列表 (例如, RuleGroupId-1:NONE, RuleGroupId-2:COUNT)。

fmsManagedToken

在您的账户中创建规则时由 AWS Firewall Manager 生成的令牌。当您创建此规则时, AWS Config 会忽略此参数。

fmsRemediationEnabled

如果为 true, 则 AWS Firewall Manager 将根据 FMS 策略更新不合规资源。当您创建此规则时, AWS Config 会忽略此参数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

iam-password-policy

检查 IAM 用户的账户密码策略是否符合指定要求。

Identifier: IAM_PASSWORD_POLICY

Trigger type: 定期

参数:

RequireUppercaseCharacters

密码中要求至少包含一个大写字符。

RequireLowercaseCharacters

密码中要求至少包含一个小写字符。

RequireSymbols

密码中要求至少包含一个符号。

RequireNumbers

密码中要求至少包含一个数字。

MinimumPasswordLength

密码最小长度。

PasswordReusePrevention

允许重用前的密码数。

MaxPasswordAge

密码到期前的天数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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

Trigger type: 配置更改

参数:

groupName

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。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

iam-user-no-policies-check

检查您的任何 IAM 用户中，没有用户拥有附加策略。IAM 用户必须继承来自 IAM 组或角色的权限。

标识符：IAM_USER_NO_POLICIES_CHECK

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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预置和维护一个同步备用副本。有关更多信息，请参阅 Amazon RDS 用户指南 中的[高可用性 \(多可用区\)](#)。

Note

此规则不评估 Amazon Aurora 数据库。

Identifier: RDS_MULTI_AZ_SUPPORT

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

rds-storage-encrypted

检查您的 RDS 数据库实例是否启用了存储加密。

Identifier: RDS_STORAGE_ENCRYPTED

Trigger type: 配置更改

参数:

kmsKeyId

用于加密存储的 KMS 密钥 ID 或 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

redshift-cluster-configuration-check

检查 Amazon Redshift 群集是否具有指定的设置。

Identifier: REDSHIFT_CLUSTER_CONFIGURATION_CHECK

Trigger type: 配置更改

参数:

clusterDbEncrypted

数据库加密已启用。

nodeTypes

指定节点类型。

loggingEnabled

审核日志记录已启用。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

redshift-cluster-maintenancesettings-check

检查 Amazon Redshift 群集是否具有指定的维护设置。

Identifier: REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

Trigger type: 配置更改

参数:

allowVersionUpgrade

允许版本升级已启用。

preferredMaintenanceWindow

为群集计划的维护时段 (例如, 周一 09:30 - 周一 10:00)。

automatedSnapshotRetentionPeriod

自动快照要被保留的天数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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 EC2 实例是否具有“CostCenter”标签。用英文逗号分隔多个值。

Identifier: REQUIRED_TAGS

Trigger type: 配置更改

参数:

tag1Key

所需标签的键。

tag1Value

所需标签的可选值。用英文逗号分隔多个值。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则, 请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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。此规则仅适用于 IPv4。

Identifier: RESTRICTED_INCOMING_TRAFFIC

Trigger type: 配置更改

参数:

blockedPort1

已阻止的 TCP 端口号。

blockedPort2

已阻止的 TCP 端口号。

blockedPort3

已阻止的 TCP 端口号。

blockedPort4

已阻止的 TCP 端口号。

blockedPort5

已阻止的 TCP 端口号。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

restricted-ssh

检查所用安全组是否不允许受限传入 SSH 流量。此规则仅适用于 IPv4。

Identifier: INCOMING_SSH_DISABLED

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

root-account-mfa-enabled

检查您的 AWS 账户的用户是否需要使用 Multi-Factor Authentication (MFA) 设备用根凭证登录。

Identifier: ROOT_ACCOUNT_MFA_ENABLED

Trigger type: 定期

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

s3-bucket-logging-enabled

检查您的 S3 存储桶是否已启用日志记录。

Identifier: S3_BUCKET_LOGGING_ENABLED

Trigger type: 配置更改

参数:

targetBucket

用于存储服务器访问日志的目标 S3 存储桶。

targetPrefix

用于存储服务器访问日志的目标 S3 存储桶的前缀。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

s3-bucket-public-read-prohibited

检查您的 Amazon S3 存储桶是否允许公有读取访问。如果 Amazon S3 存储桶策略或存储桶 ACL 允许公有读取访问，则存储桶不合规。

标识符：S3_BUCKET_PUBLIC_READ_PROHIBITED

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

s3-bucket-public-write-prohibited

检查您的 Amazon S3 存储桶是否允许公有写入访问。如果 Amazon S3 存储桶策略或存储桶 ACL 允许公有写入访问，则存储桶不合规。

标识符：S3_BUCKET_PUBLIC_WRITE_PROHIBITED

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

s3-bucket-server-side-encryption-enabled

检查 S3 存储桶策略是否拒绝未使用 AES-256 或 AWS KMS 加密的 S3:PutObject 请求。

标识符：S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

s3-bucket-ssl-requests-only

检查 S3 存储桶是否具有需要请求使用安全套接字层 (SSL) 的策略。

标识符: S3_BUCKET_SSL_REQUESTS_ONLY

Trigger type: 配置更改

参数:

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

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。

Identifier: S3_BUCKET_VERSIONING_ENABLED

Trigger type: 配置更改

参数:

isMfaDeleteEnabled

已经为您的 S3 存储桶启用了 MFA 删除。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅[使用 AWS CloudFormation 模板创建 AWS Config 托管规则 \(p. 56\)](#)。

查看	启动
查看	

使用 AWS 托管规则

您可以从 AWS 管理控制台、AWS CLI 或 AWS Config API 设置和激活 AWS 托管规则。

设置和激活 AWS 托管规则（控制台）

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在 AWS 管理控制台 菜单上，验证区域选择器是否设置为支持 AWS Config 规则的区域。有关支持区域的列表，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。
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. 如果您的规则的触发类型包括 Configuration changes，请针对 Scope of changes 指定以下选项之一以便 AWS Config 按其调用您的 Lambda 函数：
 - Resources – 当与指定资源类型（或类型和标识符）匹配的资源被创建、更改或删除时。
 - Tags – 当具有指定标签的资源被创建、更改或删除时。
 - All changes – 当 AWS Config 记录的资源被创建、更改或删除时。
 - c. 如果您的规则的触发类型包括 Periodic，请指定 Frequency，以便 AWS Config 按其调用您的 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。您的新规则将显示在 Rules 页面中。

在 AWS Config 获得您的规则的评估结果之前，Compliance 将显示 Evaluating...。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，您可能在 Compliance 中看到以下一项内容：

- No results reported - AWS Config 根据规则评估了您的资源。规则不适用于其范围内的 AWS 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 - AWS Config 无法对照规则来评估您记录的 AWS 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，或者使用 Settings 页添加 AWS Config 要记录的资源。
- Evaluations failed - 如需获得可帮助您确定问题的信息，请选择规则名称以打开其详细页面并查看错误消息。

设置和激活 AWS 托管规则 (AWS CLI)

- 使用 `put-config-rule` 命令。

设置和激活 AWS 托管规则 (AWS Config API)

- 使用 `PutConfigRule` 操作。

使用 AWS CloudFormation 模板创建 AWS Config 托管规则

对于支持的 AWS Config 托管规则，您可以使用 AWS CloudFormation 模板为账户创建规则或更新现有 AWS 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 AWS Config 托管规则。模板仅创建规则，而不创建其他 AWS 资源。

Note

在更新 AWS 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 AWS CloudFormation 模板的更多信息，请参阅 AWS CloudFormation 用户指南 中的 [AWS CloudFormation 入门](#)。

为 AWS Config 托管规则启动 AWS CloudFormation 堆栈

1. 从[AWS 托管配置规则 \(p. 28\)](#)列表中选择一个规则。
2. 选择 View 下载模板或选择 Launch Stack。如果您选择 Launch Stack，请跳至步骤 4。
3. 转至 [CloudFormation 控制台](#) 并创建新堆栈。
4. 对于 Select Template :
 - 如果您已下载模板，请选择 Upload a template to Amazon S3，然后选择 Browse 以上传模板。
 - 如果您已选择 Launch Stack 按钮，模板 URL 将自动显示在 Specify an Amazon S3 template URL 字段中。
5. 选择 Next。
6. 对于 Specify Details，键入堆栈名并输入 AWS 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”。
7. 选择 Next。
8. 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。
9. 选择 Next。
10. 对于 Review，验证模板、参数和其他选项是否正确。
11. 选择 Create。将在几分钟内创建堆栈。您可以在 [AWS Config 控制台](#) 中查看已创建的规则。

您可以使用模板为 AWS 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 AWS CloudFormation 用户指南 中的 [使用堆栈](#)。

为 AWS Config 制定自定义规则

您可以开发自定义规则并将其添加至 AWS Config。您可以将每个自定义规则与 AWS Lambda 函数相关联，函数中包含用于评估您的 AWS 资源是否符合规则的逻辑。

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 AWS Config。

[自定义规则入门 \(p. 57\)](#) 中的练习可以逐步引导您首次创建自定义规则。其中包含不加修改就可以添加至 AWS Lambda 的示例函数。

要了解 AWS Lambda 函数的原理以及如何编写这种函数，请参阅 [AWS Lambda Developer Guide](#)。

主题

- [自定义规则入门 \(p. 57\)](#)
- [为 AWS Config 制定自定义规则 \(p. 59\)](#)
- [针对 AWS Config 规则的 AWS Lambda 函数和事件示例 \(p. 62\)](#)

自定义规则入门

本程序将引导您完成自定义规则的创建流程，该规则可以评估您的各个 EC2 实例是否为 t2.micro 类型实例。AWS Config 将针对这一规则运行基于事件的评估，这意味着 AWS Config 每次检测到实例配置的更改时，都会检查您的实例配置。AWS Config 会将 t2.micro 实例标记为合规实例，并将其他所有实例标记为不合规实例。合规性状态将显示在 AWS Config 控制台中。

为保证这一程序的最佳效果，您的 AWS 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。

要创建本规则，您首先需要在 AWS Lambda 控制台中自定义一个蓝图，从而创建一个 AWS Lambda 函数。然后，您需要在 AWS Config 中创建一个自定义规则，并将此规则与函数相关联。

为您的自定义规则创建 AWS Lambda 函数

1. 通过以下网址登录 AWS 管理控制台并打开 AWS Lambda 控制台：<https://console.aws.amazon.com/lambda/>。
2. 在 AWS 管理控制台 菜单上，验证区域选择器是否设置为支持 AWS Config 规则的区域。有关支持区域的列表，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。
3. 在 AWS Lambda 控制台中，选择 Create a Lambda function。
4. 在 Select blueprint 页面，对于 filter，请键入 config-rule-change-triggered。选择筛选结果中的蓝图。
5. 在 Configure triggers 页面上，选择 Next。
6. 在 Configure function 页面，完成以下步骤：
 - a. 对于 Name，请键入 **InstanceTypeCheck**。
 - b. 对于 Runtime，请保留 Node.js。
 - c. 对于 Code entry type，请保留 Edit code inline。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。
 - d. 对于 Handler，请保留 **index.handler**。
 - e. 对于 Role，请选择 Create new role from template(s)。
 - f. 对于 Role name，请输入名称。
 - g. 对于 Policy templates，请选择 AWS Config Rules permission。
 - h. 在 Configure function 页面，选择 Next。
 - i. 在 Review 页面，验证您的函数的详细信息，然后选择 Create function。AWS 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 Actions，然后选择 Configure test event。
 - b. 在 Input test event 窗口中，对于 Sample event template，选择 AWS Config Change Triggered Rule。

- c. 选择 Save and test。AWS Lambda 会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：

```
{
  "errorMessage": "Result Token provided is invalid",
  "errorType": "InvalidResultTokenException",
  . . .
}
```

此处预期为 `InvalidResultTokenException`，因为仅当您的函数从 AWS Config 收到结果令牌时，它才能成功运行。结果令牌可以识别 AWS 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 AWS Config 所需的权限。否则，将出现这种错误消息：`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支持 `config:PutEvaluations` 操作，然后再次测试您的函数。

将您的自定义规则添加至 AWS Config

1. 使用 <https://console.aws.amazon.com/config/> 打开 AWS Config 控制台。
2. 在 AWS 管理控制台 菜单中，验证区域选择器中的区域是否与您为自定义规则创建 AWS Lambda 函数时使用的区域相同。
3. 在 Rules 页面，选择 Add rule。
4. 在 Add rule 页面，选择 Add custom rule。
5. 在 Configure rule 页面，完成以下步骤：

- a. 对于 Name，请键入 **InstanceTypesAreT2micro**。
- b. 对于 Description，请键入 **Evaluates whether EC2 instances are the t2.micro type**。
- c. 对于 AWS Lambda function ARN，请指定 AWS Lambda 分配给您的函数的 ARN。

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。AWS 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。AWS Lambda 对最新版本使用 `$LATEST` 限定词。

- d. 对于 Trigger type，请选择 Configuration changes。
- e. 对于 Scope of changes，请选择 Resources。
- f. 对于 Resources，请选择 Instance。
- g. 在 Rule parameters 部分中，您必须指定 AWS Lambda 函数评估的规则参数和需要的值。本程序中的函数会评估 `desiredInstanceType` 参数。

对于 Key，请键入 **desiredInstanceType**。对于 Value，请键入 **t2.micro**。

6. 选择 Save。您的新规则将显示在 Rules 页面中。

在 AWS Config 从您的 AWS Lambda 函数接收评估结果之前，Compliance 将会显示 Evaluating...。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 - AWS Config 根据规则评估了您的资源。规则不适用于其范围内的 AWS 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。

请验证范围中包含 Resources 的 Instance，然后重试。

- No resources in scope - AWS Config 无法对照规则来评估您记录的 AWS 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，或者使用 Settings 页添加 AWS Config 要记录的资源。
请检查确认 AWS Config 是否在记录 EC2 实例。
- Evaluations failed -如需获得可帮助您确定问题的信息，请选择规则名称以打开其详细页面并查看错误消息。

如果您的规则正常运行并且 AWS 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 \(p. 69\)](#)。

为 AWS Config 制定自定义规则

完成以下程序创建自定义规则。要创建自定义规则，您首先要创建一个 AWS Lambda 函数，其中包含该规则的评估逻辑。然后，将该函数与您在 AWS Config 创建的自定义规则关联。

内容

- [为自定义 Config 规则创建 AWS Lambda 函数 \(p. 59\)](#)
- [在 AWS Config 中创建自定义规则 \(p. 60\)](#)
- [评估其他资源类型 \(p. 61\)](#)

为自定义 Config 规则创建 AWS Lambda 函数

Lambda 函数是您上传到 AWS Lambda 的自定义代码，由事件源发布给它的事件调用。如果 Lambda 函数与 Config 规则关联，那么 AWS Config 会在发生触发规则的情况时调用该函数。之后，Lambda 函数会评估由 AWS Config 发送的配置信息，并返回评估结果。有关 Lambda 函数的更多信息，请参阅 AWS Lambda Developer Guide 中的 [函数和事件源](#)。

您可以使用 AWS Lambda 支持的编程语言为自定义规则创建一个 Lambda 函数。为简化这一任务，您可以自定义一个 AWS Lambda 蓝图，或者重复使用 AWS Config Rules GitHub 存储库中的示例函数。

AWS Lambda 蓝图

AWS 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：

- config-rule-change-triggered – 在您的 AWS 资源配置发生更改时触发。
- config-rule-periodic – 按照您选择的频率触发（例如，每 24 小时）。

AWS Config Rules 的 GitHub 存储库

我们在 GitHub 上提供了一个自定义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 AWS 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 AWS Lambda 函数中。要查看存储库，请访问 <https://github.com/aws-labs/aws-config-rules/>。

为您的自定义规则创建函数

1. 通过以下网址登录 AWS 管理控制台并打开 AWS Lambda 控制台：<https://console.aws.amazon.com/lambda/>。
2. 在 AWS 管理控制台 菜单上，验证区域选择器是否设置为支持 AWS Config 规则的区域。有关支持区域的列表，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。
3. 选择 Create a Lambda function。
4. 在 Select blueprint 页面，您可以为 AWS Config 规则选择一个蓝图函数并继续操作，也可以选择 Skip，不使用蓝图。

5. 在 Configure triggers 页面上，选择 Next。
6. 在 Configure function 页面，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 Edit code inline。
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 AWS Config 调用您的函数时，您的代码可以评估 AWS Config 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 AWS 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，AWS Config 会传递 JSON 格式的规则参数。您在 AWS Config 中创建自定义规则时，可以定义传递哪个规则参数。
 - 有关 AWS Config 在调用您的函数时发布的事件的示例，请参阅 [AWS Config 规则的示例事件 \(p. 67\)](#)。
10. 对于 Handler，请为您的函数指定处理程序。如果您正在使用蓝图，请保留默认值。
11. 对于 Role，请选择 Create new role from template(s)。
12. 对于 Role name，请输入名称。
13. 对于 Policy templates，请选择 AWS Config Rules permission。
14. 在 Configure function 页面，选择 Next。
15. 在 Review 页面，验证您的函数的详细信息，然后选择 Create function。

在 AWS Config 中创建自定义规则

使用 AWS Config 创建自定义规则并将其与 Lambda 函数关联。

创建自定义规则

1. 使用 <https://console.aws.amazon.com/config/> 打开 AWS Config 控制台。
2. 在 AWS 管理控制台 菜单中，验证区域选择器中的区域是否与您为自定义规则创建 AWS Lambda 函数时使用的区域相同。
3. 在 Rules 页面，选择 Add rule。
4. 在 Add rule 页面，选择 Add custom rule。
5. 在 Configure rule 页面，键入一个名称和描述。
6. 对于 AWS Lambda function ARN，请指定 AWS Lambda 分配给您的函数的 ARN。

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。AWS 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。AWS 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：
 - Configuration changes – AWS Config 在检测到配置更改时调用您的 Lambda 函数。
 - Periodic – AWS Config 按照您选择的频率调用您的 Lambda 函数（例如，每 24 小时）。
8. 如果您的规则的触发类型包括 Configuration changes，请针对 Scope of changes 指定以下选项之一以便 AWS Config 按其调用您的 Lambda 函数：
 - Resources – 当与指定资源类型（或类型和标识符）匹配的资源被创建、更改或删除时。
 - Tags – 当具有指定标签的资源被创建、更改或删除时。
 - All changes – 当 AWS Config 记录的资源被创建、更改或删除时。

9. 如果您的规则的触发类型包括 Periodic，请指定 Frequency，以便 AWS Config 按其调用您的 Lambda 函数。
10. 在 Rule parameters 部分，指定您的 AWS Lambda 函数评估的任何规则参数及需要的值。
11. 选择 Save。您的新规则将显示在 Rules 页面中。

在 AWS Config 从您的 AWS Lambda 函数接收评估结果之前，Compliance 将会显示 Evaluating…。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，您可能在 Compliance 中看到以下一项内容：

- No results reported - AWS Config 根据规则评估了您的资源。规则不适用于其范围内的 AWS 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 - AWS Config 无法对照规则来评估您记录的 AWS 资源，因为您的任何资源都不在规则范围内。您可以在 Settings 页面选择 AWS Config 要记录哪些资源。
- Evaluations failed - 如需获得可帮助您确定问题的信息，请选择规则名称以打开其详细页面并查看错误消息。

Note

当您使用 AWS Config 控制台创建自定义规则时，系统会自动为您创建适当权限。如果您使用 AWS CLI 创建自定义规则，您需要授予 AWS Config 权限用以调用您的 Lambda 函数。[aws lambda add-permission](#) 有关更多信息，请参阅 AWS Lambda Developer Guide 中的[对 AWS Lambda 使用基于资源的策略 \(Lambda 函数策略\)](#)。

评估其他资源类型

您可以创建自定义规则来针对 AWS Config 不记录的资源类型运行评估。如果您想评估 AWS Config 目前未记录的其他资源类型的合规性，如 Amazon Glacier 文件库或 Amazon SNS 主题，这很有用。有关您可以使用自定义规则评估的其他资源类型的列表，请参阅[AWS 资源类型参考](#)。

Note

AWS CloudFormation 用户指南中的列表可能包含最近添加，但尚不可用于在 AWS Config 中创建自定义规则的资源类型。不受支持的资源类型的完整列表如下所示。

- AWS::Batch::ComputeEnvironment
- AWS::Batch::JobDefinition
- AWS::Batch::JobQueue
- AWS::EC2::EgressOnlyInternetGateway
- AWS::EC2::SubnetCidrBlock
- AWS::EC2::VPCcidrBlock
- AWS::EMR::InstanceFleetConfig
- AWS::EMR::SecurityConfiguration
- AWS::SSM::Association
- AWS::SSM::Parameter

示例

1. 您想在您的账户中评估 Amazon Glacier 文件库。AWS Config 目前未记录 Amazon Glacier 文件库资源。
2. 您可以创建一个 AWS Lambda 函数，评估您的 Amazon Glacier 文件库是否符合您的账户要求。

3. 创建一个名为 `evaluate-glacier-vaults` 的自定义规则，然后将您的 AWS Lambda 函数分配给该规则。
4. AWS Config 调用您的 Lambda 函数，然后按照您的规则评估 Amazon Glacier 文件库。
5. AWS 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 AWS Config 时间线中的配置详细信息，并在 AWS Config 支持的资源的 AWS Config 控制台中查找资源。如果您配置 AWS 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、配置项和关系](#) (p. 6)。

针对 AWS Config 规则的 AWS Lambda 函数和事件示例

每个自定义 Config 规则均与一个 AWS Lambda 函数相关联，其中后者是包含对应规则评估逻辑的自定义代码。当 Config 规则被触发时（例如，当 AWS Config 检测到配置变更时），AWS Config 会通过发布一个事件来调用该规则的 Lambda 函数，其中事件是一个 JSON 对象，用于提供此函数评估的配置数据。

有关 AWS Lambda 中函数和事件的更多信息，请参阅 AWS Lambda Developer Guide 中的 [函数和事件源](#)。

主题

- [用于 AWS Config 规则 \(Node.js\) 的示例 AWS Lambda 函数](#) (p. 62)
- [AWS Config 规则的示例事件](#) (p. 67)

用于 AWS Config 规则 (Node.js) 的示例 AWS Lambda 函数

AWS Lambda 会在 AWS 服务发布事件时执行函数。用于自定义 Config 规则的函数会接收一个由 AWS Config 发布的事件，然后该函数使用它从事件接收以及它从 AWS Config API 检索的数据，来评估是否符合规则。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 AWS Lambda 函数常见模式的信息，请参阅 AWS Lambda Developer Guide 中的 [编程模型](#)。

内容

- [评估由配置更改触发时的示例函数](#) (p. 62)
- [定期评估时的示例函数](#) (p. 65)

评估由配置更改触发时的示例函数

AWS 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 AWS Config 控制台来创建与类似示例的函数关联的规则，请将触发类型选择为配置更改。如果您使用 AWS Config API 或 AWS CLI 来创建规则，请将 `MessageType` 属性设置为 `ConfigurationItemChangeNotification` 和 `OversizedConfigurationItemChangeNotification`。这些设置可使您的规则在每次 AWS 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 AWS 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. 当 AWS Lambda 将 event 对象传递至 handler 函数时，本函数运行。AWS Lambda 还会传递 context 对象，其中包含本函数在运行时可以使用的信息和方法。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。
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 AWS 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。如果两个值一致，则函数返回 COMPLIANT；如果不一致，则函数返回 NON_COMPLIANT。

5. 处理程序初始化 putEvaluationsRequest 对象，准备向 AWS Config 发送评估结果。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，该令牌可以识别 AWS Config 的规则和事件。
6. 处理程序向 config 客户端的 putEvaluations 方法传递对象，从而向 AWS Config 发送评估结果。

定期评估时的示例函数

AWS Config 针对定期评估调用的函数示例如下。定期评估按您在 AWS Config 中定义规则时指定的频率进行。

如果您使用 AWS Config 控制台来创建与类似示例的函数关联的规则，请将触发类型选择为定期。如果您使用 AWS Config API 或 AWS CLI 来创建规则，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. 当 AWS Lambda 将 event 对象传递至 handler 函数时，本函数运行。AWS Lambda 还会传递 context 对象，其中包含本函数在运行时可以使用的信息和方法。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。
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 config 客户端的 listDiscoveredResources 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. 处理程序初始化 putEvaluationsRequest 对象，准备向 AWS Config 发送评估结果。该对象包含 Evaluations 参数，该参数可以识别合规性结果和在事件中发布的 AWS 账户。您可以使用 Evaluations 参数将结果应用到 AWS 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，该令牌可以识别 AWS 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. 处理程序向 config 客户端的 putEvaluations 方法传递对象，从而向 AWS Config 发送评估结果。

AWS Config 规则的示例事件

当规则被触发时，AWS Config 会通过发布一个事件来调用该规则的 AWS Lambda 函数。然后，AWS 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 AWS 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": "{\n\"configurationItem\":{\n\"configurationItemCaptureTime\":  
\"2016-02-17T01:36:34.043Z\", \n\"awsAccountId\": \"123456789012\", \n\"configurationItemStatus\":  
\"OK\", \n\"resourceId\": \"i-00000000\", \n\"ARN\": \"arn:aws:ec2:us-east-2:123456789012:instance/  
i-00000000\", \n\"awsRegion\": \"us-east-2\", \n\"availabilityZone\": \"us-east-2a\",  
\"resourceType\": \"AWS::EC2::Instance\", \n\"tags\": {\n\"Foo\": \"Bar\"}, \n\"relationships\":  
[\n{\n\"resourceId\": \"eipalloc-00000000\", \n\"resourceType\": \"AWS::EC2::EIP\", \n\"name\":  
\"Is attached to ElasticIp\"}, \n\"configuration\": {\n\"foo\": \"bar\"}, \n\"messageType\":  
\"ConfigurationItemChangeNotification\"}\n]\",  
  "ruleParameters": "{\n\"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\\\": \\\"8flee69b287895a0f8bc5753eca68e96\\\", \\\"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 AWS 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

AWS 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 AWS 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 \(p. 81\)](#) 中的 get-resource-config-history AWS 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 AWS Config 控制台创建自定义规则时，您可以定义参数。您也可以使用 PutConfigRule AWS Config API 请求或 put-config-rule AWS CLI 命令中的 InputParameters 属性来定义参数。

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 AWS Config 的令牌。

eventLeftScope

表明要评估的 AWS 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 PutEvaluations 调用中的 ComplianceType 属性值来忽略评估。

executionRoleArn

分配给 AWS Config 的 IAM 角色的 ARN。

configRuleArn

AWS Config 分配给规则的 ARN。

configRuleName

您向导致 AWS Config 发布事件并调用函数的规则分配的名称。

configRuleId

AWS Config 分配给规则的 ID。

accountId

拥有规则的 AWS 账户的 ID。

version

AWS 分配的版本号。如果 AWS 向 AWS 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。

AWS Config 事件的当前版本为 1.0。

查看配置合规性

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

查看合规性（控制台）

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在 AWS 管理控制台 菜单上，验证区域选择器是否设置为支持 AWS Config 规则的区域。有关支持区域的列表，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。
3. 在导航窗格中，选择 Rules。控制台将显示 Rules 页面，其中列出了您的规则及每个规则的合规性状态。
4. 选择一个规则，以查看它的 Rule details 页面。此页面将显示该规则的配置、状态及任何不符合该规则的 AWS 资源。
5. 如果 Rule details 显示任何不合规资源，请针对资源选择 Config timeline 图标 (⌂)，以查看其配置时间线页面。当 AWS Config 检测到资源不合规时，该页面将显示其记录的配置设置。此信息可帮

助您确定资源不符合规则的原因。有关更多信息，请参阅 [在 AWS Config 控制台中查看配置详细信息 \(p. 79\)](#)。

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 AWS Config 发现的资源 \(p. 78\)](#)。

Example 查看合规性 (AWS CLI)

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，AWS Config 将通过 CappedCount 参数返回不合规资源的数量。

- 要查看 AWS 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-nnnnnnnnn",
          "ConfigRuleName": "ConfigRuleName"
        }
      },
      "ResultRecordedTime": 1443751424.969,
      "ConfigRuleInvokedTime": 1443751421.208,
      "ComplianceType": "COMPLIANT"
    },
    {
      "EvaluationResultIdentifier": {
        "OrderingTimestamp": 1443610576.349,
        "EvaluationResultQualifier": {
          "ResourceType": "AWS::EC2::Instance",
          "ResourceId": "i-nnnnnnnnn",

```

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

- 要查看每个特定类型的 AWS 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-nnnnnnnnn",
      "Compliance": {
        "ComplianceContributorCount": {
          "CappedCount": 1,
          "CapExceeded": false
        },
        "ComplianceType": "NON_COMPLIANT"
      }
    },
    {
      "ResourceType": "AWS::EC2::Instance",
      "ResourceId": "i-nnnnnnnnn",
      "Compliance": {
        "ComplianceType": "COMPLIANT"
      }
    }
  ],
  ...
}
```

- 要查看单个 AWS 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-nnnnnnnnn
{
  "EvaluationResults": [
    {
      "EvaluationResultIdentifier": {
        "OrderingTimestamp": 1443610576.349,
        "EvaluationResultQualifier": {
          "ResourceType": "AWS::EC2::Instance",
          "ResourceId": "i-nnnnnnnnn",
          "ConfigRuleName": "instances-in-vpc"
        }
      },
      "ResultRecordedTime": 1443751425.083,
      "ConfigRuleInvokedTime": 1443751421.301,
      "ComplianceType": "NON_COMPLIANT"
    }
  ]
}
```

Example 查看合规性 (AWS Config API)

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 `DescribeComplianceByConfigRule` 操作。

- 要查看 AWS 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 AWS 资源的合规性状态，请使用 [DescribeComplianceByResource](#) 操作。
- 要查看单个 AWS 资源的合规性详细信息，请使用 [GetComplianceDetailsByResource](#) 操作。详细信息包括：用于评估资源的 AWS 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。

管理您的 AWS Config 规则

您可以使用 AWS Config 控制台、AWS CLI 和 AWS Config API 来查看、添加和删除您的规则。

内容

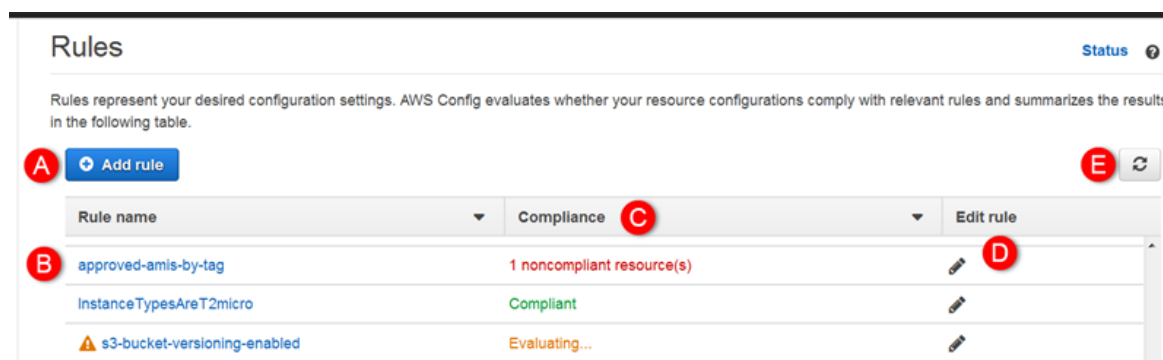
- [使用控制台](#) (p. 72)
- [使用 AWS CLI](#) (p. 74)
- [使用 AWS Config API](#) (p. 75)
- [删除评估结果](#) (p. 76)

使用控制台

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 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在 AWS 管理控制台中，验证区域选择器是否设置为支持 AWS Config 规则的区域。有关支持区域的列表，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。
3. 选择 Rules。Rules 页面显示了您的规则以及每个规则的合规性状态。



- A. 选择 Add rule 以开始创建规则。
- B. 选择规则名称以查看其设置。
- C. 当规则评估资源时，请查看规则的合规性状态。
- D. 选择 Edit rule 图标 () 以编辑规则。
- E. 选择“刷新”() 图标以重新加载合规性结果。

更新规则

1. 针对您要更新的规则，选择 Edit rule 图标 (🔧)。
2. 在 Config rule 页面上修改设置，以根据需要更改您的规则。
3. 选择 Save。

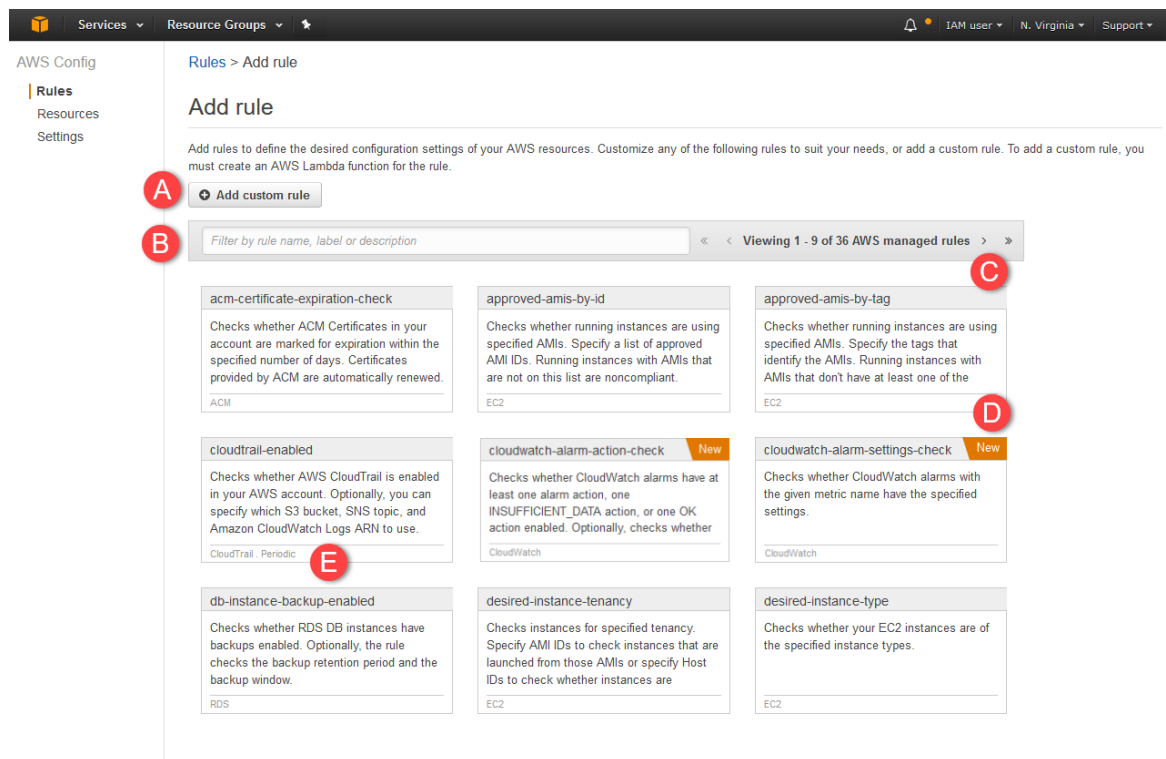
删除一项规则

1. 针对您要删除的规则，选择 Edit rule 图标 (🔧)。
2. 在 Configure rule 页面上，选择 Delete rule。
3. 系统提示时，选择 Delete。

添加一项规则

如果您选择 Add rule，可以在 Add rule 页面上查看可用的 AWS 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，然后按照为 [AWS Config 制定自定义规则 \(p. 59\)](#) 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 [AWS 托管规则 \(p. 55\)](#) 中的过程操作。



在 Add rule 页面上，可以执行以下操作：

- A. 选择 Add custom rule 以创建自己的规则。

- B. 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 [AWS Config 规则指定触发器 \(p. 26\)](#)。
- C. 选择箭头图标可查看下一页规则。
- D. 最近添加的规则标记为 New。
- E. 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。

使用 AWS CLI

查看您的规则

- 使用 `describe-config-rules` 命令：

```
$ aws configservice describe-config-rules
```

AWS 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。要参考您的规则的详细信息，可使用 `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 AWS 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
```

使用 AWS Config API

查看您的规则

使用 `DescribeConfigRules` 操作。

更新或添加规则

使用 `PutConfigRule` 操作。

删除一项规则

使用 `DeleteConfigRule` 操作。

删除评估结果

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 \(p. 77\)](#)。

手动评估您的资源

您可以使用 AWS Config 手动按照 AWS Config 规则评估您的资源或删除评估结果。

内容

- [评估您的资源 \(p. 76\)](#)
- [删除评估结果 \(p. 77\)](#)

评估您的资源

当您创建自定义规则或使用托管规则时，AWS 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 AWS Config 是否正确评估您的资源或确定 AWS Lambda 函数的评估逻辑是否有问题时，这很有用。

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. AWS 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。

手动评估您的资源（控制台）

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在 AWS 管理控制台 菜单上，验证区域选择器是否设置为支持 AWS Config 规则的区域。有关支持区域的列表，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。
3. 在导航窗格中，选择 Rules。Rules 页面显示了您的规则以及每个规则的合规性状态。
4. 从列表中选择规则。
5. 在 Re-evaluate rule 部分，选择 Re-evaluate。
6. AWS 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 AWS 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。

手动评估您的资源 (AWS CLI)

- 使用 start-config-rules-evaluation 命令。

```
$ aws configservice start-config-rules-evaluation --config-rule-names ConfigRuleName
```

AWS 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
```

手动评估您的资源 (AWS Config API)

- 使用 [StartConfigRulesEvaluation](#) 操作。

删除评估结果

AWS Config 评估您的规则后，您可以在该规则 Rules 页或 Rules details 页上查看评估结果。如果评估结果不正确，或者如果您要重新评估，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。

手动删除评估结果（控制台）

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在 AWS 管理控制台 菜单上，验证区域选择器是否设置为支持 AWS Config 规则的区域。有关支持区域的列表，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。
3. 在导航窗格中，选择 Rules。Rules 页面显示了您的规则以及合规性状态。
4. 从列表中选择规则。
5. 在 Delete evaluation results 部分，选择 Delete results。AWS Config 删除此规则的评估结果。
6. 系统提示时，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。

手动删除评估结果 (AWS CLI)

- 使用 delete-evaluation-results 命令：

```
$ aws configservice delete-evaluation-results --config-rule-name ConfigRuleName
```

AWS Config 删除规则的评估结果。

手动删除评估结果 (AWS Config API)

- 使用 [DeleteEvaluationResults](#) 操作。

查看 AWS 资源配置和历史记录

您可以查看 AWS 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。您可以使用 AWS Config 控制台或 AWS CLI 并按其中的步骤操作。

主题

- [查找 AWS Config 发现的资源 \(p. 78\)](#)
- [在 AWS Config 控制台中查看配置详细信息 \(p. 79\)](#)
- [使用 CLI 查看配置详细信息 \(p. 81\)](#)
- [来自 AWS Config 的示例 Amazon EBS 配置历史记录。 \(p. 83\)](#)
- [来自 AWS Config 的配置快照示例 \(p. 86\)](#)
- [AWS Config 发送的通知 \(p. 90\)](#)


查找 AWS Config 发现的资源

您可以使用 AWS Config 控制台、AWS CLI 和 AWS Config API 来查找 AWS Config 获取或发现的资源，包括已删除的资源 and AWS Config 目前未记录的资源。AWS 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 AWS 资源类型 \(p. 6\)](#)。

查找资源 (AWS Config 控制台)

您可以使用资源类型或标签信息在 AWS Config 控制台中查找资源。

查找资源

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在 资源清单 页上，为您要查找的资源指定搜索选项：
 - 选择 资源，然后在列表选择一个或多个资源类型。此列表包含 AWS Config 支持的资源类型。要缩小结果范围，请在下一个框中键入资源 ID，或资源名称（如适用）。您还可以选择 包括已删除资源。
 - 选择 标签，然后键入应用于您的资源的标签键，例如 **CostCenter**。要缩小结果范围，请在下一个框中输入标签值。
3. 在指定搜索选项后，选择 Look up。
4. AWS 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：
 - Resource identifier – 资源标识符可以是资源 ID，也可以是资源名称（如果适用）。选择资源标识符链接可在该服务的控制台中查看该资源。例如，选择 EC2 实例的资源标识符会将您转到 Amazon EC2 控制台。
 - Compliance – AWS Config 按照您的规则评估的资源的状态。
 - Config timeline – Config 时间线  显示资源的配置详细信息的历史记录。选择该图标以查看该资源的详细信息页面。有关更多信息，请参阅 [在 AWS Config 控制台中查看配置详细信息 \(p. 79\)](#)。

查找资源 (AWS CLI)

您可以使用 AWS CLI 列出 AWS Config 发现的资源。

查找资源 (AWS CLI)

- 使用 `aws configservice list-discovered-resources` 命令：

Example

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

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。有关此命令及 AWS Config 响应的示例，请参阅 [查看配置历史记录 \(p. 81\)](#)。

查找资源 (AWS Config API)


您指定资源类型后，AWS Config 将返回该类型资源的资源标识符列表。有关详细信息，请在 AWS Config API Reference 中查看 [ResourceIdentifier](#)。

查找资源 (AWS Config API)

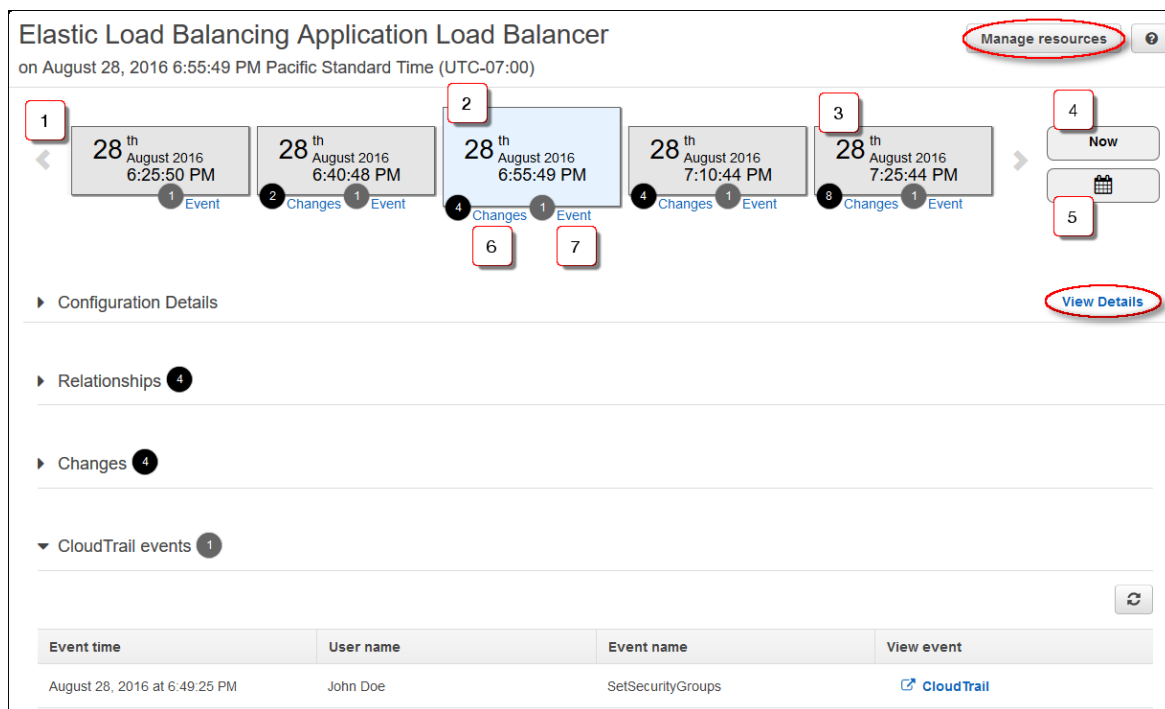
- 使用 `ListDiscoveredResources` 操作。

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。

在 AWS Config 控制台中查看配置详细信息

当您在 [资源清单](#) 页上查找资源时，您可以选择 Config 时间线 ，用以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。

页面顶部的块统称为时间线。时间线显示了记录的创建日期和时间。



详细信息页面的功能

1. 单击以将时间线滚动至资源配置历史记录中更早的时间点。
2. 单击某个时间线块以选择该时间段。配置详细信息、关系和更改部分中的描述涵盖了所选时间段内选定资源的配置项。
3. 显示最近的配置更改。
4. 单击以使时间线返回至当前时间。
5. 通过指定日期（以及时间，如果需要）来查看配置项，然后选择应用。
6. 单击以导航至更改部分。Changes 后面的数字是该资源在所选时间段与前一个块指示的时间段之间发生的配置更改次数。
7. 单击以导航到 CloudTrail events 部分。Events 后面的数字是该资源在所选时间段与前一个块指示的时间段之间发生的 API 事件数量。您可以看到过去 7 天 AWS CloudTrail 记录到 API 事件。过去 7 天前发生的 CloudTrail 事件不能在时间线中查看。

有关更多信息，请参阅 AWS CloudTrail User Guide 中的[使用 CloudTrail API 活动历史记录查看事件](#)。

Note

CloudTrail 活动可能由于以下原因而不可用：

- 验证您对 CloudTrail 拥有足够的读取权限。有关更多信息，请参阅[只读权限示例 \(p. 133\)](#)。
- 出现服务问题，CloudTrail 事件此时无法显示。请尝试刷新页面。
- 您在此区域中没有 CloudTrail 跟踪，或您的跟踪未启用日志记录。有关更多信息，请参阅 AWS CloudTrail User Guide 中的[首次创建跟踪](#)。

所选资源的时间线导航提示

以下是使用时间线查看有关所选资源的信息的提示。

- 使用时间线任意一端的箭头查看在其他时间段记录的配置项的时间线块。

- 选择 **配置详细信息** 查看选定资源的描述。
- 选择 **关系** 查看此账户中与选定资源相关的受支持资源的列表。如果 **关系** 部分没有展开，则表示选定资源在所选时间段内与您账户中存在的其他资源都不相关。

有关更多信息，请参阅 [资源关系 \(p. 3\)](#)。

- 如果显示所选时间段内存在更改，请选择 **更改** 查看对该资源所作的配置更改。Changes 部分还会列出因配置更改而产生的关系更改。
- 选择 **CloudTrail events** 查看有关涉及资源的 API 调用的信息，如事件时间、用户名和事件名称。例如，如果 AWS Config 正在记录 IAM 资源类型，而且 IAM 角色已更新，您可以查看事件以了解 Event name 中的 UpdateRole。
- 在 View event 列中，您还可以选择 CloudTrail 链接以在 CloudTrail 控制台中查看关于事件的更多信息。您必须创建跟踪并对 CloudTrail 启用日志记录，才能查看 AWS Config 时间线中的事件。
- 选择 **查看详细信息** 查看以文本或 JSON 格式列出的配置信息。单击详细信息窗口中的箭头以查看其他详细信息。

有关详细信息窗口中条目的更多信息，请参阅 [配置项的组成部分 \(p. 9\)](#)。

- 选择 **Manage resources** 以转到选定资源的控制台。如果您对资源进行了更改，请返回 AWS Config 控制台，然后选择 **现在** 查看相应更改。此过程将花费 10 分钟刷新资源的详细信息页面。

控制台还会提供有关您未列入 AWS Config 记录的资源列表中的受支持资源的详细信息页面。这些详细信息页面上的信息是有限的，且不会显示正在进行的配置更改。

使用 CLI 查看配置详细信息

AWS 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。AWS Config 还会定期将配置项作为配置历史记录传递到指定的传递通道。

您可以使用 AWS CLI 查看每个资源的配置项历史记录，并传递和查看配置快照。

主题

- [查看配置历史记录 \(p. 81\)](#)
- [传送配置快照 \(p. 82\)](#)

查看配置历史记录

您可以使用 AWS CLI 来查看各种资源配置的历史记录。请使用 `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": "{\n  \"ownerId\": \"605053316265\", \"groupName\": \"default\n\", \"groupId\": \"sg-6fbb3807\", \"description\": \"default group\", \"ipPermissions\":\n  [{\n    \"ipProtocol\": \"tcp\", \"fromPort\": 80, \"toPort\": 80, \"userIdGroupPairs\": [{\n      \"userId\n\": \"amazon-elb\", \"groupName\": \"amazon-elb-sg\", \"groupId\": \"sg-843f59ed\"}],\n    \"ipRanges\": [{\n      \"0.0.0.0/0\"}],\n    \"ipProtocol\": \"tcp\", \"fromPort\": 0, \"toPort\": 65535,\n    \"userIdGroupPairs\": [{\n      \"userId\": \"605053316265\", \"groupName\": \"default\", \"groupId\n\": \"sg-6fbb3807\"}],\n    \"ipRanges\": [],\n    \"ipProtocol\": \"udp\", \"fromPort\": 0, \"toPort\n\": 65535, \"userIdGroupPairs\": [{\n      \"userId\": \"605053316265\", \"groupName\": \"default\",\n      \"groupId\": \"sg-6fbb3807\"}],\n    \"ipRanges\": [],\n    \"ipProtocol\": \"icmp\", \"fromPort\": -1,\n    \"toPort\": -1, \"userIdGroupPairs\": [{\n      \"userId\": \"605053316265\", \"groupName\": \"default\n\", \"groupId\": \"sg-6fbb3807\"}],\n    \"ipRanges\": [],\n    \"ipProtocol\": \"tcp\", \"fromPort\n\": 1433, \"toPort\": 1433, \"userIdGroupPairs\": [],\n    \"ipRanges\": [{\n      \"0.0.0.0/0\"}],\n    \"ipProtocol\n\": \"tcp\", \"fromPort\": 3389, \"toPort\": 3389, \"userIdGroupPairs\": [],\n    \"ipRanges\":\n  [{\n    \"207.171.160.0/19\"}],\n    \"ipPermissionsEgress\": [],\n    \"vpcId\": null, \"tags\": []}],\n  \"configurationItemStatus\": \"ResourceDiscovered\",\n  \"accountId\": \"605053316265\"
}
",
"nextToken":
.....

```

有关响应字段的详细解释，请参阅 [配置项的组成部分 \(p. 9\)](#) 和 [支持的资源关系 \(p. 11\)](#)。

传送配置快照

AWS Config 可以向您在配置传递通道时指定的 Amazon S3 存储桶传送 AWS Config 记录的 AWS 资源的配置项。

传送配置快照

- 当您配置了传递通道时，请通过指定由 AWS Config 分配的名称来使用 `deliver-config-snapshot` 命令，例如：

```

$ aws configservice deliver-config-snapshot --delivery-channel-name default
{
    "configSnapshotId": "94ccff53-83be-42d9-996f-b4624b3c1a55"
}

```

下一步是验证配置快照是否成功传送到传递通道。

验证传送状态

- 请使用 `describe-delivery-channel-status` 命令验证 AWS 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 AWS 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 `configSnapshotDeliveryInfo` 中的 `lastSuccessfulTime` 字段。时间应与您上次请求传送配置快照的时间一致。

Note

AWS Config 使用 UTC 格式 (GMT-08:00) 来记录时间。

查看您的 Amazon S3 存储桶中的配置快照

- 登录 AWS 管理控制台并通过以下网址打开 Amazon S3 控制台：<https://console.aws.amazon.com/s3/>。
- 在 Amazon S3 控制台的全局 Buckets 列表中，单击您的 Amazon S3 存储桶的名称。
- 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 存储桶中还包含一个名为 `ConfigWritabilityCheckFile` 的空文件。AWS Config 创建该文件的目的是验证服务能否成功写入 S3 存储桶。

来自 AWS Config 的示例 Amazon EBS 配置历史记录。

AWS Config 生成一组文件，每个文件均代表一个资源类型，并列出 AWS Config 正在记录的相应类型的资源的所有配置更改。AWS Config 会将此以资源为中心的配置历史记录导出为您在启动 AWS Config 时指定的 Amazon S3 存储桶中的对象。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 AWS 账户的当前区域中所有 Amazon Elastic Block Store 卷的配置历史记录。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"
      ],
      "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": [
          {
            "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"
],
"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": [
    {
      "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"
  ],
  "availabilityZone": "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"
}
]
```

来自 AWS Config 的配置快照示例

当您调用 [DeliverConfigSnapshot](#) 操作或运行 AWS CLI `deliver-config-snapshot` 命令时，AWS Config 会生成配置快照。AWS Config 会将配置快照存储在您启用 AWS Config 时指定的 Amazon S3 存储桶中。

下面是 AWS Config 在配置快照中提供的信息示例。该快照描述了 AWS Config 在当前区域中为您的 AWS 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"
],
"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": [
    {
      "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"
  ],
  "availabilityZone": "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
}
]
```

AWS Config 发送的通知

您可以将 AWS Config 配置为将配置变更和通知流式传输到 Amazon SNS 主题。例如，在资源更新时，您可以通过电子邮件接收通知，从而能够查看变更。您也可以在 AWS Config 针对您的资源评估自定义规则或托管规则时收到通知。

AWS 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。
- AWS Config 未能向您的账户传输通知。

Note

如果您选择电子邮件作为 SNS 主题的通知终端节点，则会产生大量电子邮件。

主题

- [通过电子邮件监控 AWS Config 资源变更 \(p. 90\)](#)
- [示例配置项变更通知 \(p. 94\)](#)
- [示例配置历史记录传输通知 \(p. 101\)](#)
- [示例配置快照传输开始通知 \(p. 102\)](#)
- [示例配置快照传输通知 \(p. 102\)](#)
- [示例合规性变更通知 \(p. 103\)](#)
- [示例规则评估开始通知 \(p. 104\)](#)
- [示例过大配置项变更通知 \(p. 105\)](#)
- [示例传输失败通知 \(p. 105\)](#)

通过电子邮件监控 AWS Config 资源变更

如果您已将 AWS Config 设置为将配置变更和通知流式传输到 Amazon SNS 主题，则可通过电子邮件监控这些变更。这些电子邮件中可能包含配置历史记录、规则合规性、快照信息和变更通知。您也可以基于主题行或邮件正文设置电子邮件筛选条件，以查找特定变更。

通过邮件电子监控资源变更

1. 如果您尚未执行此操作，请对 AWS Config 进行设置以将通知传递到 Amazon SNS 主题。有关更多信息，请参阅 [使用控制台设置 AWS Config \(p. 15\)](#) 或 [使用 AWS CLI 设置 AWS Config \(p. 19\)](#)。
2. 通过以下网址打开 Amazon SNS 控制台：<https://console.aws.amazon.com/sns/v2/home>。

3. 在 Amazon SNS 控制台的导航窗格中，选择 Topics。
4. 在 Topics 页面上，打开您在设置 AWS Config 时指定的 Amazon SNS 主题，方法是选择其在 ARN 列中的名称。
5. 在 Topic details 页面上，选择 Subscriptions 下的 Create subscription。
6. 在 Create Subscription 对话框中，为 Protocol 选择 Email。
7. 对于 Endpoint，键入您要发送通知的电子邮件地址。
8. 选择 Create subscription。

查看您的电子邮件是否有电子邮件确认。同时，控制台会在 Subscription ID 列中显示 PendingConfirmation。

9. 打来自“AWS 通知”的电子邮件，然后选择 Confirm subscription。

Tip

如果您想监控特定资源或其他重要变更，则可在电子邮件应用程序中设置电子邮件筛选条件。

电子邮件格式和筛选条件示例

如果您创建了对 Amazon SNS 主题的电子邮件订阅，则可以按照主题行和消息正文中的信息筛选您接收到的电子邮件。要创建对 Amazon SNS 主题的订阅，请参阅 [通过电子邮件监控 AWS Config 资源变更 \(p. 90\)](#)。

电子邮件的主题行如下示例所示：

```
[AWS Config:us-west-2] AWS::EC2::Instance i-12abcd3e Created in Account 123456789012
```

在电子邮件客户端应用程序中，您可以设置电子邮件筛选条件或规则，以查看特定更改或整理您收到的通知。例如，您可以按区域、资源类型、资源名称或 AWS 账户来整理电子邮件通知。电子邮件筛选条件可以帮助您管理来自多个账户的通知或您账户中的很多资源。

电子邮件订阅的消息正文通过 Email 协议创建，其中包含与您的 AWS 资源的创建、更新和删除事件相关的信息。以下示例显示了一份通过 Email 协议创建的电子邮件消息正文。此通知包含针对资源的配置项变更。

```
View the Timeline for this Resource in AWS Config Management Console:
https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/AWS::
EC2::Instance/i-12abcd3e
```

New State and Change Record:

```
-----
{
  "configurationItemDiff": {
    "changedProperties": {},
    "changeType": "CREATE"
  },
  "configurationItem": {
    "configurationItemVersion": "1.0",
    "configurationItemCaptureTime": "2015-03-19T21:20:35.737Z",
    "configurationStateId": 1,
    "relatedEvents": [
      "4f8abc4f-6def-4g42-hi03-46j3b48k0lmn"
    ],
    "awsAccountId": "123456789012",
    "configurationItemStatus": "ResourceDiscovered",
    "resourceId": "i-92aeda5b",
    "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/i-12abcd3e",
    "awsRegion": "us-west-2",
    "availabilityZone": "us-west-2c",
    "configurationStateMd5Hash": "123456789e0f930642026053208e",
```



```

"resourceType": "AWS::EC2::Instance",
"resourceCreationTime": "2015-03-19T21:13:05.000Z",
"tags": {},
"relationships": [
  {
    "resourceId": "abc-1234de56",
    "resourceType": "AWS::EC2::NetworkInterface",
    "name": "Contains NetworkInterface"
  },
  {
    "resourceId": "ab-cl2defg3",
    "resourceType": "AWS::EC2::SecurityGroup",
    "name": "Is associated with SecurityGroup"
  },
  {
    "resourceId": "subnet-a1b2c3d4",
    "resourceType": "AWS::EC2::Subnet",
    "name": "Is contained in Subnet"
  },
  {
    "resourceId": "vol-a1bc234d",
    "resourceType": "AWS::EC2::Volume",
    "name": "Is attached to Volume"
  },
  {
    "resourceId": "vpc-a12bc345",
    "resourceType": "AWS::EC2::VPC",
    "name": "Is contained in Vpc"
  }
],
"configuration": {
  "instanceId": "i-12abcd3e",
  "imageId": "ami-123a4567",
  "state": {
    "code": 16,
    "name": "running"
  },
  "privateDnsName": "ip-000-00-0-000.us-west-2.compute.internal",
  "publicDnsName":
"ec2-12-345-678-910.us-west-2.compute.amazonaws.com",
  "stateTransitionReason": "",
  "keyName": null,
  "amiLaunchIndex": 0,
  "productCodes": [],
  "instanceType": "t2.micro",
  "launchTime": "2015-03-19T21:13:05.000Z",
  "placement": {
    "availabilityZone": "us-west-2c",
    "groupName": "",
    "tenancy": "default"
  },
  "kernelId": null,
  "ramdiskId": null,
  "platform": null,
  "monitoring": {
    "state": "disabled"
  },
  "subnetId": "subnet-a1b2c3d4",
  "vpcId": "vpc-a12bc345",
  "privateIpAddress": "000.00.0.000",
  "publicIpAddress": "00.000.000.000",
  "stateReason": null,
  "architecture": "x86_64",
  "rootDeviceType": "ebs",
  "rootDeviceName": "/dev/abcd",
  "blockDeviceMappings": [

```

```

    {
      "deviceName": "/dev/abcd",
      "ebs": {
        "volumeId": "vol-a1bc234d",
        "status": "attached",
        "attachTime": "2015-03-19T21:13:07.000Z",
        "deleteOnTermination": true
      }
    }
  ],
  "virtualizationType": "hvm",
  "instanceLifecycle": null,
  "spotInstanceRequestId": null,
  "clientToken": "ab1234c5-6d78-910-1112-13ef14g15hi16",
  "tags": [],
  "securityGroups": [
    {
      "groupName": "default",
      "groupId": "sg-a12bcde3"
    }
  ],
  "sourceDestCheck": true,
  "hypervisor": "xen",
  "networkInterfaces": [
    {
      "networkInterfaceId": "eni-1234ab56",
      "subnetId": "subnet-a1b2c3d4",
      "vpcId": "vpc-a12bc345",
      "description": "",
      "ownerId": "123456789012",
      "status": "in-use",
      "macAddress": "1a:23:45:67:b8",
      "privateIpAddress": "000.00.0.000",
      "privateDnsName": "ip-000-00-0-000.us-west-2.compute.internal",
      "sourceDestCheck": true,
      "groups": [
        {
          "groupName": "default",
          "groupId": "sg-a12bcde3"
        }
      ],
      "attachment": {
        "attachmentId": "eni-attach-123a4b5c",
        "deviceIndex": 0,
        "status": "attached",
        "attachTime": "2015-03-19T21:13:05.000Z",
        "deleteOnTermination": true
      },
      "association": {
        "publicIp": "00.000.000.000",
        "publicDnsName":
"ec2-00-000-000-000.us-west-2.compute.amazonaws.com",
        "ipOwnerId": "amazon"
      },
      "privateIpAddresses": [
        {
          "privateIpAddress": "000.00.0.000",
          "privateDnsName":
"ip-000-00-0-000.us-west-2.compute.internal",
          "primary": true,
          "association": {
            "publicIp": "00.000.000.000",
            "publicDnsName":
"ec2-000-00-0-000.us-west-2.compute.amazonaws.com",
            "ipOwnerId": "amazon"
          }
        }
      ]
    }
  ]
}

```

```
    }
  ]
}
],
"iamInstanceProfile": null,
"ebsOptimized": false,
"sriovNetSupport": null
}
},
"notificationCreationTime": "2015-03-19T21:20:36.808Z",
"messageType": "ConfigurationItemChangeNotification",
"recordVersion": "1.2"
}
```

示例配置项变更通知

AWS 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传输状态，并提供 AWS Config 在记录的 AWS 资源的配置发生更改时创建的每个配置项。AWS Config 还会发送显示您的资源与规则是否相符的通知。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。当 AWS Config 检测到 Amazon Elastic Block Store 卷 vol-ce676ccc 挂载到 ID 为 i-344c463d 的实例时，会生成这一通知。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",
  "configurationItems": [
    {
      "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": [
        "06c12a39-eb35-11de-ae07-adb69edbb1e4",
        "c376e30d-71a2-4694-89b7-a5a04ad92281"
      ],
      "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/whAzT2lVtofc365En2TlNcd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedsIzC6KxkfWTFXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqgomYDjc5h0kgapIo4CtC
+qZhMzEbHWpzFlEzvFl55KaZXDbznBD1ZkqPgno/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 AWS Config 如何为存在关系的资源创建配置项。

1. 比如您有一个 ID 为 i-007d374c8912e3e90 的 Amazon EC2 实例，该实例与 Amazon EC2 安全组 sg-c8b141b4 关联。
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 AWS 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": ["e61e1419-7cb0-477f-8dde-bbfe27467a96"],
    "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": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHL1C
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUGTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNT009xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4S132bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX61qlDZ79w==",
"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": ["e61e1419-7cb0-477f-8dde-bbfe27467a96"],
      "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 AWS 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/
RJQiCPsCNfG0J0rUZlrfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUnlAie/
yeGFduc6P3EotP3zt02rhmxjezf3c1lurstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/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 AWS Config 在 AWS 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/jumOMBsgRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPux//
olSJ4neWallBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjnlEv7PlZqxmT+ux3SR/
C54cbfcdUdpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm+H9wavcwXB9XECelHhRW70Y
+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO+81ceAXIg2E1m7hZ71z4PA==",
  "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 AWS 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+ROsshg5G+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 AWS Config 针对您的自定义规则或托管规则评估您的资源时，AWS 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
+6gcttHCRVlhNemzp/
YmBmTfO6azYXt0FJDaeVd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSZcQyERgkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqslDhbgWYnp3c80mVLl7ohP4hilcxdyWAgXrbsN32ekYr15gdHozx8
+BI221ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "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

AWS 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 AWS 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+ItYlLFkE9jACSB13sQ1uSjYzEhEbN7Cs
+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 AWS 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，则通知中会包含配置项的简短摘要。您可以在 `s3BucketLocation` 字段中指定的 Amazon S3 存储桶位置中查看完整通知。

下面的示例通知显示了 Amazon EC2 实例的一个配置项。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 AWS Config Management 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

如果 AWS Config 无法向您的 Amazon S3 存储桶传输配置快照或过大配置项变更通知，AWS Config 会发送传输失败通知。请确认您指定了有效的 Amazon S3 存储桶。

View the Timeline for this Resource in AWS Config Management 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:

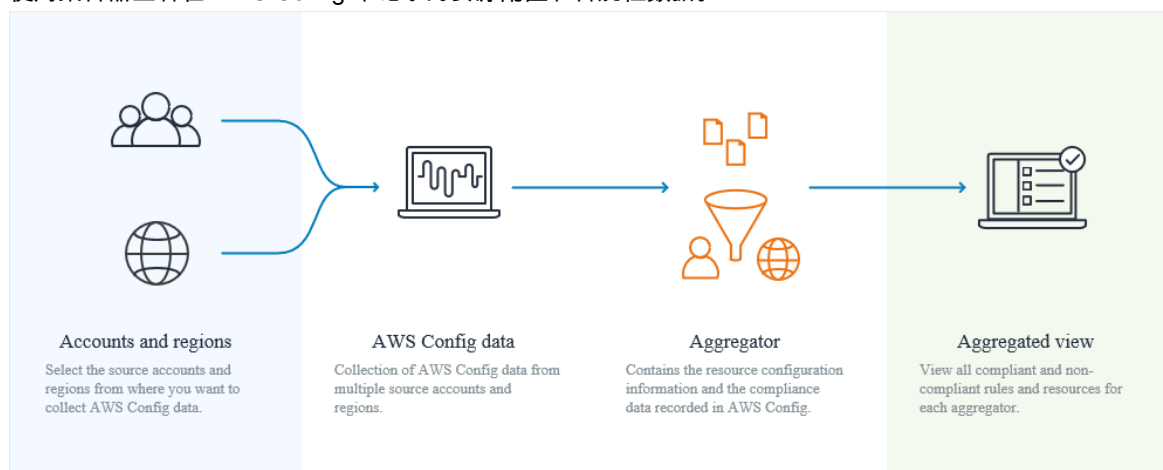
```
-----  
{  
  "configurationItemSummary": {  
    "changeType": "UPDATE",  
    "configurationItemVersion": "1.2",  
    "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",  
    "configurationStateId": 0,  
    "awsAccountId": "123456789012",  
    "configurationItemStatus": "OK",  
    "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"  
}
```

多账户多区域数据聚合

聚合器是一种 AWS Config 资源类型，用于从以下内容收集 AWS Config 数据：

- 多个账户和多个区域。
- 单个账户和多个区域。
- AWS Organizations 中的组织和该组织中的所有账户。

使用聚合器查看在 AWS Config 中记录的资源配置和合规性数据。



有关概念的更多信息，请参阅“概念”主题中的[多账户多区域数据聚合 \(p. 3\)](#)部分。

要从源账户和区域收集您的 AWS Config 数据，请从以下操作开始：

1. 添加聚合器以聚合多个账户和区域的 AWS Config 数据。
2. 授权聚合账户收集 AWS Config 数据。当源账户是单个账户时，需要授权。如果要聚合的源账户是 AWS Organizations 的一部分，则不需要授权。
3. 在聚合视图中监控规则和账户的合规性数据。

主题

- [使用控制台设置聚合器 \(p. 107\)](#)
- [使用 AWS Command Line Interface 设置聚合器 \(p. 109\)](#)
- [使用控制台授权聚合器账户来收集 AWS Config 数据 \(p. 113\)](#)
- [使用 AWS Command Line Interface 授权聚合器账户来收集 AWS Config 数据 \(p. 115\)](#)
- [在聚合视图中查看合规性数据 \(p. 116\)](#)
- [多账户多区域数据聚合的故障排除 \(p. 118\)](#)

使用控制台设置聚合器

在 Aggregator 页面上，可以执行以下操作：

- 通过指定要从中聚合数据的源账户 ID 或组织和区域来创建聚合器。
- 编辑和删除聚合器。

主题

- [添加聚合器 \(p. 108\)](#)
- [编辑聚合器 \(p. 109\)](#)
- [删除聚合器 \(p. 109\)](#)
- [了解更多 \(p. 109\)](#)

添加聚合器

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 导航到 Aggregators 页面，然后选择 Add aggregator。
3. Allow data replication，授予 AWS Config 权限，使其可将数据从源账户复制到聚合器账户中。

选择 Allow AWS Config to replicate data from source account(s) into an aggregator account. You must select this checkbox to continue to add an aggregator。

4. 对于 Aggregator name，键入聚合器的名称。

聚合器名称必须是唯一的名称，最多有 64 个字母数字字符。此名称可以包含连字符和下划线。

5. 对于 Select source accounts，选择您要从中聚合数据的 Add individual account IDs 或 Add my organization。

- 如果您选择 Add individual account IDs，则可以为聚合器账户添加个人账户 ID。

1. 选择 Add source accounts 以添加账户 ID。

2. 选择 Add AWS account IDs 以手动添加逗号分隔的 AWS 账户 ID。如果您想要从当前账户中聚合数据，请键入账户的账户 ID。

OR

选择 Upload a file 以上传以逗号分隔的 AWS 账户 ID 的文件 (.txt 或 .csv)。

3. 选择 Add source accounts 以确认您的选择。

- 如果您选择 Add my organization，则可以将您组织中的所有账户添加到聚合器账户。

Note

您必须登录到主账户，并且所有功能都必须在组织中处于启用状态。此选项会自动在 AWS Config 和 AWS Organizations 之间[启用集成](#)。

1. 选择 Choose IAM role 以创建一个 IAM 角色或从您的账户中选择一个现有 IAM 角色。

您必须分配 IAM 角色以允许 AWS Config 为您的组织调用只读 API。

2. 选择 Create a role，然后键入 IAM 角色名称以创建 IAM 角色。

OR

选择 Choose a role from your account 以选择现有的 IAM 角色。

Note

在 IAM 控制台中，将 AWSConfigRoleForOrganizations 托管策略附加到您的 IAM 角色。附加此策略能让 AWS Config 调用 AWS Organizations DescribeOrganization、ListAWSServiceAccessForOrganization 和 ListAccounts API。您必须编辑控制策略文档以包含 config.amazonaws.com 可信实体。

3. 选择 Choose IAM role 以确认您的选择。

6. 对于 Regions，选择您要为其聚合数据的区域。

- 选择一个区域或多个区域或所有 AWS 区域。
 - 选择 Include future AWS regions 以从启用了多账户多区域数据聚合的所有未来 AWS 区域中聚合数据。
7. 选择 Save。AWS Config 会显示聚合器。

编辑聚合器

1. 要对聚合器进行更改，请选择聚合器名称。
2. 选择 Actions，然后选择 Edit。
3. 使用 Edit aggregator 页面上的所需部分来更改聚合器的源账户、IAM 角色或区域。

Note

您无法将源类型从个人账户更改为组织，反之亦然。

4. 选择 Save。

删除聚合器

1. 要删除聚合器，请选择聚合器名称。
2. 选择 Actions，然后选择 Delete。

此时会显示一条警告消息。删除聚合器会导致所有聚合数据丢失。您无法恢复此数据，但数据源账户不受影响。

3. 选择 Delete 以确认您的选择。

了解更多

- [概念 \(p. 2\)](#)
- [使用控制台授权聚合器账户来收集 AWS Config 数据 \(p. 113\)](#)
- [在聚合视图中查看合规性数据 \(p. 116\)](#)
- [多账户多区域数据聚合的故障排除 \(p. 118\)](#)

使用 AWS Command Line Interface 设置聚合器

您可以使用 AWS Command Line Interface (AWS CLI) 创建、查看、更新和删除 AWS Config 聚合器数据。要使用 AWS 管理控制台，请参阅[使用控制台设置聚合器 \(p. 107\)](#)。

AWS CLI 是用于管理 AWS 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 AWS 服务并使用脚本来自动执行这些服务。

要在本地计算机上安装 AWS CLI，请参阅 AWS CLI 用户指南中的[安装 AWS CLI](#)。

如有必要，键入 `aws configure` 将配置 AWS CLI 为以使用一个提供 AWS Config 聚合器的 AWS 区域。

主题

- [使用个人账户添加聚合器 \(p. 110\)](#)
- [使用 AWS 组织添加聚合器 \(p. 111\)](#)

- [查看聚合器 \(p. 111\)](#)
- [编辑聚合器 \(p. 112\)](#)
- [删除聚合器 \(p. 113\)](#)
- [了解更多 \(p. 109\)](#)

使用个人账户添加聚合器

1. 打开命令提示符或终端窗口。
2. 键入以下命令以创建一个名为 **MyAggregator** 的聚合器。

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

对于 account-aggregation-sources，请键入以下命令之一。

- 以逗号分隔的您要为其聚合数据的 AWS 账户 ID 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}]")。
- 您还可以上传以逗号分隔的 AWS 账户 ID 的 JSON 文件。上传文件使用以下语法：`--account-aggregation-sources MyFilePath/MyFile.json`

JSON 文件必须为以下格式：

```
[
  {
    "AccountIds": [
      "AccountID1",
      "AccountID2",
      "AccountID3"
    ],
    "AllAwsRegions": true
  }
]
```

3. 按 Enter 执行命令。

您应该可以看到类似于如下所示的输出内容：

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:us-east-2:123456789101:config-
aggregator/config-aggregator-floppus3",
    "CreationTime": 1517942461.442,
    "ConfigurationAggregatorName": "MyAggregator",
    "AccountAggregationSources": [
      {
        "AllAwsRegions": true,
        "AccountIds": [
          "AccountID1",
          "AccountID2",
          "AccountID3"
        ]
      }
    ],
    "LastUpdatedTime": 1517942461.442
  }
}
```

```
}
```

使用 AWS 组织添加聚合器

1. 打开命令提示符或终端窗口。
2. 键入以下命令以创建一个名为 **MyAggregator** 的聚合器。

```
aws configservice put-configuration-aggregator --configuration-aggregator-name  
MyAggregator --organization-aggregation-source "{\"RoleArn\": \"Complete-Arn\",  
\"AllAwsRegions\": true}"
```

3. 按 Enter 执行命令。

您应该可以看到类似于如下所示的输出内容：

```
{  
  "ConfigurationAggregator": {  
    "ConfigurationAggregatorArn": "arn:aws:config:us-east-2:123456789101:config-  
aggregator/config-aggregator-floppus3",  
    "CreationTime": 1517942461.442,  
    "ConfigurationAggregatorName": "MyAggregator",  
    "OrganizationAggregationSource": {  
      "AllAwsRegions": true,  
      "RoleArn": "arn:aws:config:us-east-2:123456789101:config-aggregator/  
config-aggregator-floppus3"  
    },  
    "LastUpdatedTime": 1517942461.442  
  }  
}
```

查看聚合器

1. 键入以下命令：

```
aws configservice describe-configuration-aggregators
```

2. 根据您的源账户，您应该看到类似于以下内容的输出：

对于个人账户

```
{  
  "ConfigurationAggregators": [  
    {  
      "ConfigurationAggregatorArn": "arn:aws:config:us-  
east-2:123456789101:config-aggregator/config-aggregator-floppus3",  
      "CreationTime": 1517942461.442,  
      "ConfigurationAggregatorName": "MyAggregator",  
      "AccountAggregationSources": [  
        {  
          "AllAwsRegions": true,  
          "AccountIds": [  
            "AccountID1",  
            "AccountID2",  
            "AccountID3"  
          ]  
        }  
      ]  
    }  
  ],  
}
```

```
        "LastUpdatedTime": 1517942461.455
      }
    ]
  }
}
```

OR

对于组织

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:us-east-2:123456789101:config-agggregator/config-aggregator-floppus3",
    "CreationTime": 1517942461.442,
    "ConfigurationAggregatorName": "MyAggregator",
    "OrganizationAggregationSource": {
      "AllAwsRegions": true,
      "RoleArn": "arn:aws:config:us-east-2:123456789101:config-aggregator/config-aggregator-floppus3"
    },
    "LastUpdatedTime": 1517942461.442
  }
}
```

编辑聚合器

1. 您可以使用 `put-configuration-aggregator` 命令来更新或编辑配置聚合器。

键入以下命令以向 **MyAggregator** 添加新的账户 ID：

```
aws configservice put-configuration-aggregator --configuration-aggregator-name
MyAggregator --account-aggregation-sources "[{\"AccountIds\": [\"AccountID1\",
\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"
```

2. 根据您的源账户，您应该看到类似于以下内容的输出：

对于个人账户

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:us-east-2:123456789101:config-agggregator/config-aggregator-xz2upuu6",
    "CreationTime": 1517952090.769,
    "ConfigurationAggregatorName": "MyAggregator",
    "AccountAggregationSources": [
      {
        "AllAwsRegions": true,
        "AccountIds": [
          "AccountID1",
          "AccountID2",
          "AccountID3",
          "AccountID4"
        ]
      }
    ],
    "LastUpdatedTime": 1517952566.445
  }
}
```

OR

对于组织

```
{
  "ConfigurationAggregator": {
    "ConfigurationAggregatorArn": "arn:aws:config:us-east-2:123456789101:config-aggregator/config-aggregator-floppus3",
    "CreationTime": 1517942461.442,
    "ConfigurationAggregatorName": "MyAggregator",
    "OrganizationAggregationSource": {
      "AllAwsRegions": true,
      "RoleArn": "arn:aws:config:us-east-2:123456789101:config-aggregator/config-aggregator-floppus3"
    },
    "LastUpdatedTime": 1517942461.442
  }
}
```

删除聚合器

使用 AWS CLI 删除配置聚合器

- 键入以下命令：

```
aws configservice delete-configuration-aggregator --configuration-aggregator-name
MyAggregator
```

如果成功，则命令会执行，而没有附加输出。

了解更多

- [概念 \(p. 2\)](#)
- [使用 AWS Command Line Interface 授权聚合器账户来收集 AWS Config 数据 \(p. 115\)](#)
- [在聚合视图中查看合规性数据 \(p. 116\)](#)
- [多账户多区域数据聚合的故障排除 \(p. 118\)](#)

使用控制台授权聚合器账户来收集 AWS Config 数据

AWS Config 能让您授权聚合器账户来收集 AWS Config 数据。

如果要聚合的源账户是 AWS Organizations 的一部分，则不需要此流。

在 Authorizations 页面上，可以执行以下操作：

- 添加授权以允许聚合器账户和区域收集 AWS Config 数据。
- 授权聚合器账户的某个待处理请求来收集 AWS Config 数据。
- 删除对聚合器账户的授权。

主题

- [为聚合器账户和区域添加授权 \(p. 114\)](#)

- 授权针对聚合器账户的待处理请求 (p. 114)
- 删除对现有聚合器账户的授权 (p. 115)
- 了解更多 (p. 109)

为聚合器账户和区域添加授权

您可以添加授权以向聚合器账户和区域授予收集 AWS Config 数据的权限。

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 导航到 Authorizations 页面，然后选择 Add authorization。
3. 对于 Aggregator account，键入聚合器账户的 12 位数账户 ID。
4. 对于 Aggregator region，选择允许聚合器账户在其中收集 AWS Config 数据的 AWS 区域。
5. 选择 Add authorization 以确认您的选择。

AWS Config 会显示聚合器账户、区域和授权状态。

Note

您还可以使用 AWS CloudFormation 示例模板以编程方式向聚合器账户和区域编程添加授权。有关更多信息，请参阅 AWS CloudFormation user guide 中的 [AWS::Config::AggregationAuthorization](#)。

授权针对聚合器账户的待处理请求

如果您有来自现有聚合器账户的待处理授权请求，您将在 Authorizations 页面上看到请求状态。您可以从此页面授权待处理请求。

1. 对于要授权的聚合器账户，在 Actions 列中选择 Authorize。

AWS Config

Dashboard

Rules

Resources

Settings

Authorizations 1

Aggregated view

Rules

Aggregators

What's new

Learn More

Documentation

Partners

Pricing

FAQs

Authorizations

Authorize accounts to collect your AWS Config compliance and configuration data.

Hide diagram

Your AWS Config data
Authorizes aggregator accounts to collect your AWS Config compliance data and resource configuration information.

Other accounts
Accounts with aggregators that collect AWS Config data from source accounts.

Aggregators
Aggregators are AWS Config resource types that collect AWS Config data from multiple accounts and regions.

[Add authorization](#)

Account	Region	Authorization	Actions
122345566778	us-west-2	✓ Authorized	Delete
123456789012	eu-west-1	✓ Authorized	Delete
185679245380	us-west-2	✓ Authorized	Delete
123869065234	us-west-2	ⓘ Requesting for authorization	Authorize Delete

此时会显示一条确认消息，用以确认您向聚合器账户和区域授予收集 AWS Config 数据的权限。

2. 选择 Authorize 以向聚合器账户和区域授予此权限。

授权状态从 Requesting for authorization 更改为 Authorized。

删除对现有聚合器账户的授权

1. 对于要删除授权的聚合器账户，在 Actions 列中选择 Delete。

此时会显示一条警告消息。当您删除此授权后，将不会与聚合器账户共享 AWS Config 数据。

Note

在删除对聚合器的授权后，数据将保留在聚合器账户中长达 24 小时，然后才被删除。

2. 选择 Delete 以确认您的选择。

该聚合器账户被删除。

了解更多

- [概念 \(p. 2\)](#)
- [使用控制台设置聚合器 \(p. 107\)](#)
- [在聚合视图中查看合规性数据 \(p. 116\)](#)
- [多账户多区域数据聚合的故障排除 \(p. 118\)](#)

使用 AWS Command Line Interface 授权聚合器账户来收集 AWS Config 数据

您可以使用 AWS Command Line Interface (AWS CLI) 授权聚合器账户从源账户收集 AWS Config 数据和删除聚合器账户。要使用 AWS 管理控制台，请参阅[使用控制台授权聚合器账户来收集 AWS Config 数据 \(p. 113\)](#)。

AWS CLI 是用于管理 AWS 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 AWS 服务并使用脚本来自动执行这些服务。

要在本地计算机上安装 AWS CLI，请参阅 AWS CLI 用户指南中的[安装 AWS CLI](#)。

如有必要，键入 `aws configure` 将配置 AWS CLI 为以使用一个提供 AWS Config 聚合器的 AWS 区域。

主题

- [为聚合器账户和区域添加授权 \(p. 115\)](#)
- [删除授权账户 \(p. 116\)](#)
- [了解更多 \(p. 109\)](#)

为聚合器账户和区域添加授权

1. 打开命令提示符或终端窗口。
2. 键入以下命令：

```
aws configservice put-aggregation-authorization --authorized-account-id AccountID --  
authorized-aws-region Region
```


- 按 Enter。

您应该可以看到类似于如下所示的输出内容：

```
{
  "AggregationAuthorization": {
    "AuthorizedAccountId": "123456789012",
    "AggregationAuthorizationArn": "arn:aws:config:us-east-2:803981987763:aggregation-authorization/123456789012/us-east-1",
    "CreationTime": 1518116709.993,
    "AuthorizedAwsRegion": "us-east-1"
  }
}
```

删除授权账户

要使用 AWS CLI 删除授权账户

- 键入以下命令：

```
aws configservice delete-aggregation-authorization --authorized-account-id AccountID
--authorized-aws-region Region
```

如果成功，则命令会执行，而没有附加输出。

了解更多

- 概念 (p. 2)
- 使用 AWS Command Line Interface 设置聚合器 (p. 109)
- 在聚合视图中查看合规性数据 (p. 116)
- 多账户多区域数据聚合的故障排除 (p. 118)

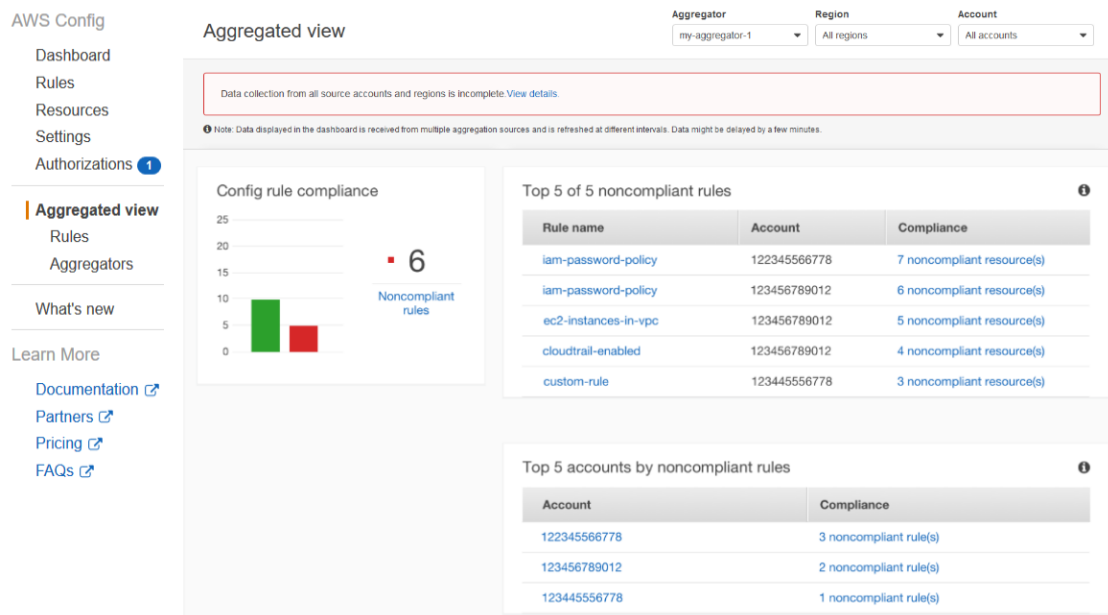
在聚合视图中查看合规性数据

Aggregated view 页面显示规则及其合规性状态的概览。它提供了合规和不合规规则的图表。不合规规则按最大数量的不合规资源和具有最大数量不合规规则的源账户排列。

一经设置，AWS Config 便会开始将指定源账户中的数据聚合到聚合器中。AWS Config 在该页面上显示规则的合规性状态可能需要几分钟的时间。

使用聚合视图

- 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
- 在导航窗格中，选择 Aggregated view，然后查看您的规则及其合规性状态。



在 Aggregated view 页面上，可以执行以下操作：

- 从 Aggregator 列表选择一个聚合器。
- 从 Region 列表选择所需区域。默认情况下，All regions 处于选中状态。
- 从 Account 列表选择一个账户。默认情况下，All accounts 处于选中状态。
- 按照不合规资源数量以降序查看前五个不合规规则。选择一个规则以转到 Rule details 页面。
- 按照不合规规则数量以降序查看前五个账户 (按不合规规则)。选择一个账户以转到 Aggregated Rules 页面。在此页面上，您可以查看所有账户的聚合规则。

Note

图块上显示的数据会发生延迟。

在聚合视图中会显示 Data collection from all source accounts and regions is incomplete 消息，原因如下：

- AWS Config 不合规规则传输正在进行中。
- AWS Config 无法找到符合筛选条件的规则。选择适当的账户或区域，然后重试。

在聚合视图中会显示 Data collection from your organization is incomplete. You can view the below data only for 24 hours. 消息，原因如下：

- 由于 IAM 角色无效，AWS Config 无法访问您的组织详细信息。如果 IAM 角色无效的时间超过 24 小时，AWS Config 将会删除整个组织的数据。
- AWS Config 服务访问在您的组织中处于禁用状态。

了解更多

- [概念 \(p. 2\)](#)
- [使用控制台设置聚合器 \(p. 107\)](#)
- [使用控制台授权聚合器账户来收集 AWS Config 数据 \(p. 113\)](#)

- [多账户多区域数据聚合的故障排除 \(p. 118\)](#)

多账户多区域数据聚合的故障排除

AWS Config 可能不会从源账户聚合数据，原因可能是以下之一：

如果发生这种情况	请执行该操作
AWS Config 在源账户中未启用。	在源账户中启用 AWS Config 并授权聚合器账户收集数据。
未给予聚合器账户授权。	登录到源账户，并授权聚合器账户以收集 AWS Config 数据。
可能存在阻止数据聚合的暂时性问题。	数据聚合可能会发生延迟。请等待几分钟。

AWS Config 可能不会从组织聚合数据，原因可能是以下之一：

如果发生这种情况	请执行该操作
由于 IAM 角色无效，AWS Config 无法访问您的组织详细信息。	创建一个 IAM 角色，或从 IAM 角色列表选择一个有效的 IAM 角色。 Note 如果 IAM 角色无效的时间超过 24 小时，AWS Config 将会删除整个组织的数据。
AWS Config 服务访问在您的组织中处于禁用状态。	您可以通过 <code>EnableAWSServiceAccess</code> API 在 AWS Config 和 AWS Organizations 之间启用集成。如果您在控制台中选择 <code>Add my organization</code> ，AWS Config 会自动在 AWS Config 和 AWS Organizations 之间启用集成。
AWS Config 无法访问您的组织详细信息，因为您的组织中未启用所有功能。	在 AWS Organizations 控制台中 启用所有功能 。

了解更多

- [概念 \(p. 2\)](#)
- [使用控制台设置聚合器 \(p. 107\)](#)
- [使用控制台授权聚合器账户来收集 AWS Config 数据 \(p. 113\)](#)
- [在聚合视图中查看合规性数据 \(p. 116\)](#)

管理 AWS Config

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 Amazon Simple Storage Service 存储桶和 Amazon Simple Notification Service 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

- [管理传递通道 \(p. 119\)](#)
- [更新分配给 AWS Config 的 IAM 角色 \(p. 121\)](#)
- [管理配置记录器 \(p. 122\)](#)
- [选择 AWS Config 所记录的资源 \(p. 124\)](#)

管理传递通道

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

每个 AWS 账户只能有一个传递通道，且使用 AWS Config 时必须使用传递通道。

更新传递通道

更新传递通道时，您可以设置以下选项：

- AWS Config 向其发送配置快照和配置历史记录文件的 Amazon S3 存储桶。
- AWS Config 将配置快照传送到 Amazon S3 存储桶的频率。
- AWS Config 向其发送关于配置更改的通知的 Amazon SNS 主题。

更新传递通道 (控制台)

- 您可以使用 AWS 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 AWS Config \(p. 15\)](#)。

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 AWS CLI、AWS Config API 或一种 AWS 软件开发工具包。

更新传递通道 (AWS 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，AWS Config 会向新传递通道分配 **default** 这一名称。

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 \(p. 120\)](#)。

- **s3BucketName** – AWS Config 向其传送配置快照和配置历史记录文件的 Amazon S3 存储桶的名称。

如果您指定的存储桶属于其他 AWS 账户，则该存储桶必须拥有授予 AWS Config 访问权限的策略。有关更多信息，请参阅 [针对 Amazon S3 存储桶的权限 \(p. 130\)](#)。

- **snsTopicARN** – AWS Config 向其发送配置更改通知的 Amazon SNS 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 AWS Config 访问权限的策略。有关更多信息，请参阅 [Amazon SNS 主题的权限 \(p. 132\)](#)。

- **configSnapshotDeliveryProperties** – 包含 **deliveryFrequency** 属性，用于设置 AWS Config 传送配置快照的频率。

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。

AWS 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 AWS CLI、AWS Config API 或一种 AWS 开发工具包。

重命名传递通道 (AWS 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
```

更新分配给 AWS Config 的 IAM 角色

您可以随时更新 AWS Config 担任的 IAM 角色。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 AWS 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 角色并将所需策略关联到 IAM 角色的信息，请参阅 [创建 IAM 角色 \(p. 21\)](#)。

Note

要查找现有 IAM 角色的 ARN，请前往 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 AWS 管理控制台 或 AWS CLI 更新您的 IAM 角色。

在支持规则的区域中更新 IAM 角色（控制台）

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

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在导航窗格中，选择 Settings。

3. 在 AWS Config role 部分，选择 IAM 角色：

- Create a role – AWS Config 创建具备所需权限的角色。对于 Role name，您可以自定义 AWS Config 创建的角色的名称。
- Choose a role from your account – 对于 Role name，从您的账户中选择一个 IAM 角色。AWS Config 将附加所需的策略。有关更多信息，请参阅 [分配给 AWS Config 的 IAM 角色权限 \(p. 128\)](#)。

Note

如果您希望按原样使用 IAM 角色，请选中该框。AWS Config 不会将策略附加到角色。

4. 选择 Save。

在不支持规则的区域中更新 IAM 角色（控制台）

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在 资源清单 页面，选择设置图标 (⚙️)。
3. 选择 继续。
4. 在 AWS Config 请求获得读取您的资源配置的许可 页面，选择 查看详细信息。
5. 在 Role Summary 部分，选择 IAM 角色：
 - 如果您想创建一个角色，对于 IAM Role，请选择 创建新的 IAM 角色。然后为 角色名称 键入名称。
 - 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 Policy Name，请选择一个可用策略，或者选择 创建新的角色策略 以创建一个策略。
6. 选择 允许。

更新 IAM 角色 (AWS 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
```

管理配置记录器

AWS 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 AWS Config 才可以跟踪资源配置。

如果您使用控制台或 AWS CLI 设置 AWS Config，AWS 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 [Getting Started With AWS Config \(p. 15\)](#)。

默认情况下，配置记录器会记录 AWS 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 AWS Config 所记录的资源 \(p. 124\)](#)。

当 AWS 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 [AWS 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 AWS Config 使用费，除非您恢复记录。

在您启动配置记录器时，AWS Config 会使用您的账户中的所有 AWS 资源的清单。

管理配置记录器（控制台）

您可以使用 AWS 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 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 在导航窗格中，选择 Settings。
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，请选择 继续。
 - 如果您要开始记录，请选择 Recording is off 下的 Turn on。系统提示时，请选择 继续。

管理配置记录器 (AWS CLI)

您可以使用 AWS CLI 停止或启动配置记录器。您还可以使用 AWS CLI、AWS Config API 或某个 AWS 软件开发工具包重命名或删除配置记录器。以下步骤可帮助您使用 AWS 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
```

选择 AWS Config 所记录的资源

AWS 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。AWS Config 会将这些事件记录为配置项。您可以自定义 AWS Config，以使其记录所有受支持类型的资源更改，或仅记录与您相关的资源类型的更改。要了解 AWS Config 可记录的资源类型，请参阅 [支持的 AWS 资源类型 \(p. 6\)](#)。

记录所有受支持的资源类型

默认情况下，AWS Config 会记录在其运行区域中发现的所有受支持类型的区域性资源的配置更改。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 AWS 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。AWS Config 支持的全局性资源类型包括 IAM 用户、组、角色和客户托管策略。

Important

一个特定全局性资源的配置详细信息在所有区域中都是相同的。如果您在多个区域自定义 AWS Config 以使其记录全局性资源，则每当全局性资源更改时，AWS Config 都会创建多个配置项：每个区域一个配置项。这些配置项将包含相同的数据。为避免配置项重复，您应考虑仅在一个区域自定义 AWS Config 以记录全局性资源，除非您希望配置项可在多个区域使用。

记录特定的资源类型

如果您不希望 AWS 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。AWS 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，AWS 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，AWS 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 AWS 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 AWS Config 停止记录某个类型的资源。在 AWS 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。

AWS Config 规则可用于仅评估那些 AWS Config 记录的资源的合规性。

选择资源 (控制台)

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

选择资源

1. 登录 AWS 管理控制台 并通过以下网址打开 AWS Config 控制台：<https://console.aws.amazon.com/config/>。
2. 打开 Settings 页面：
 - 如果您在支持 AWS Config 规则的区域中使用 AWS Config，请在导航窗格中选择 Settings。有关支持区域的列表，请参阅 Amazon Web Services 一般参考 中的 [AWS Config 区域和终端节点](#)。
 - 否则，请在 资源清单 页面选择设置图标 (⚙️)。
3. 在 Resource types to record 部分，请指定您希望 AWS Config 记录的 AWS 资源类型：
 - All resources – AWS Config 会使用下列选项记录所有受支持的资源：
 - Record all resources supported in this region – AWS Config 将记录区域性资源的每种受支持类型的配置更改。AWS 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。
 - Include global resources – AWS Config 将受支持类型的全局性资源包括在它所记录的资源（例如 IAM 资源）中。AWS 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。
 - Specific types – AWS Config 仅记录您指定的 AWS 资源类型的配置更改。
4. 保存您的更改：
 - 如果您在支持 AWS Config 规则的区域中使用 AWS Config，请选择 Save。
 - 否则，请选择 Continue。在 AWS Config 请求获得读取您的资源配置的许可 页面，请选择 允许。

选择资源 (AWS CLI)

您可以使用 AWS CLI 选择您希望 AWS 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` – AWS Config 将记录每种受支持类型的区域性资源的配置更改。AWS 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` – AWS Config 将受支持类型的全局性资源包括在它所记录的资源中。AWS 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 `aws 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 AWS 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 `allSupported` 和 `includeGlobalResourceTypes` 选项设置为 `false` 或者忽略它们，才可以为 `resourceTypes` 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"
}
]
```

用于 AWS Config 的权限

要充分使用 AWS Config，您需要创建权限策略并将其关联到您的 IAM 角色、Amazon Simple Storage Service (S3) 存储桶和 Amazon Simple Notification Service (SNS) 主题。策略是用于授予 AWS Config 权限的一组语句。下列主题提供了推荐 IAM 策略的示例，这些策略将与 AWS Config 控制台和 AWS Command Line Interface 配合使用。

主题

- [分配给 AWS Config 的 IAM 角色权限 \(p. 128\)](#)
- [针对 Amazon S3 存储桶的权限 \(p. 130\)](#)
- [Amazon SNS 主题的权限 \(p. 132\)](#)
- [AWS Config 的访问权限 \(p. 132\)](#)

分配给 AWS Config 的 IAM 角色权限

您可以通过 AWS Identity and Access Management (IAM) 角色定义一组权限。AWS Config 采用您分配给它的角色，用以写入您的 S3 存储桶、发布到您的 SNS 主题，以及进行 `Describe` 或 `List` API 请求来获取 AWS 资源的配置详细信息。有关 IAM 角色的更多信息，请参阅 IAM 用户指南 中的 [IAM 角色](#)。

当您使用 AWS Config 控制台创建或更新 IAM 角色时，AWS Config 会自动为您附加必需的权限。有关更多信息，请参阅 [使用控制台设置 AWS Config \(p. 15\)](#)。

内容

- [创建 IAM 角色策略 \(p. 128\)](#)
 - [将一项 IAM 信任策略添加到您的角色 \(p. 128\)](#)
 - [用于 Amazon S3 存储桶的 IAM 角色策略 \(p. 129\)](#)
 - [用于 Amazon SNS 主题的 IAM 角色策略 \(p. 129\)](#)
 - [用于获取配置详细信息的 IAM 角色策略 \(p. 129\)](#)
- [有关记录 S3 存储桶的疑难解答 \(p. 130\)](#)

创建 IAM 角色策略

当您使用 AWS Config 控制台创建 IAM 角色时，AWS Config 会自动为您附加该角色所需的权限。

如果您使用 AWS CLI 设置 AWS Config，或者更新一个现有 IAM 角色，您必须手动更新策略以允许 AWS Config 访问您的 S3 存储桶、发布到您的 SNS 主题，以及获取有关您资源的配置详细信息。

将一项 IAM 信任策略添加到您的角色

您可以创建一项 IAM 信任策略，让 AWS Config 可以切换到一个角色并利用其跟踪您的资源。有关信任策略的更多信息，请参阅 IAM 用户指南 中的 [代入角色](#)。

下面是 AWS 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"
  }
]
```

用于 Amazon S3 存储桶的 IAM 角色策略

以下示例策略授予 AWS Config 权限以访问您的 Amazon S3 存储桶：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:PutObject"],
      "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 "
    }
  ]
}
```

用于 Amazon SNS 主题的 IAM 角色策略

以下示例策略授予 AWS Config 权限以访问您的 SNS 主题：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sns:Publish",
      "Resource": "mySNSTopicARN"
    }
  ]
}
```

用于获取配置详细信息的 IAM 角色策略

为了记录您的 AWS 资源配置，AWS Config 需要具备 IAM 权限才能获取有关您的资源的配置详细信息。

使用 AWS 托管策略 `AWSConfigRole`，并将其附加到您分配给 AWS Config 的 IAM 角色。每次 AWS Config 添加对某个 AWS 资源类型的支持时，AWS 都会更新此策略，这意味着，只要角色附加了此托管策略，AWS Config 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，AWS Config 将为您附加 `AWSConfigRole`。

如果您使用 AWS CLI，请使用 `attach-role-policy` 命令，并为 `AWSConfigRole` 指定 Amazon 资源名称 (ARN)：

```
$ aws iam attach-role-policy --role-name myConfigRole --policy-arn arn:aws:iam::aws:policy/service-role/AWSConfigRole
```

有关记录 S3 存储桶的疑难解答

如果您已将 AWS Config 配置为记录账户的 S3 存储桶，则 AWS Config 会在创建、更新或删除 S3 存储桶时进行记录并发送通知。

如果您已将 AWS Config 配置为记录 S3 存储桶且不接收配置更改通知：

- 验证分配给 AWS Config 的 IAM 角色是否具有 `AWSConfigRole` 托管策略。
- 如果您具有已附加到存储桶的 S3 存储桶策略，请验证这些策略是否允许 AWS Config 记录对存储桶的更改。

如果您拥有 S3 存储桶的自定义策略，则可将以下策略添加到现有存储桶策略。此策略授予 AWS Config 权限以记录 S3 存储桶。

```
{
  "Sid": "AWSConfig_ReadConfiguration_Access",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::myAccountID::role/config-role"},
  "Action": [
    "s3:GetAccelerateConfiguration",
    "s3:GetBucketAcl",
    "s3:GetBucketCORS",
    "s3:GetBucketLocation",
    "s3:GetBucketLogging",
    "s3:GetBucketNotification",
    "s3:GetBucketPolicy",
    "s3:GetBucketRequestPayment",
    "s3:GetBucketTagging",
    "s3:GetBucketVersioning",
    "s3:GetBucketWebsite",
    "s3:GetLifecycleConfiguration",
    "s3:GetReplicationConfiguration"
  ],
  "Resource": "arn:aws:s3:::myBucketName"
}
```

针对 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。只有资源所有者和创建存储桶的 AWS 账户才能访问该存储桶及其包含的所有对象。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 AWS Config 自动为您创建了 S3 存储桶（例如，如果您使用 AWS Config 控制台或 `aws config subscribe` 命令设置传递通道）或者您选择了自己账户中已有的 S3 存储桶，那么这些权限将自动添加到该

S3 存储桶。但是，如果您指定的是来自其他账户的现有 S3 存储桶，则您必须确保该 S3 存储桶具有相应权限。

其他账户中的 Amazon S3 存储桶所需的权限

当 AWS Config 向您账户中的 Amazon S3 存储桶发送配置信息（历史记录文件和快照）时，它会担任您在对其进行设置时分配的 IAM 角色。当 AWS Config 向其他账户中的 S3 存储桶发送配置信息时，它会首先尝试使用 IAM 角色。但是，如果该存储桶的访问策略未向此 IAM 角色授予 WRITE 访问权限，那么此次尝试将会失败。在这种情况下，AWS Config 会再次发送这些信息，这次会以 AWS Config 服务委托人的身份发送。该访问策略必须向名称为 `config.amazonaws.com` 的委托人授予 WRITE 访问权限。这样一来，AWS Config 便会成为其向 S3 存储桶传递的对象的所有者。

授权 AWS Config 访问其他账户中的 Amazon S3 存储桶

按照以下步骤向其他账户中的 Amazon S3 存储桶添加访问策略。该访问策略允许 AWS Config 向该存储桶发送配置信息。

1. 使用该 S3 存储桶所属的账户登录 AWS 管理控制台。
2. 通过以下网址打开 Amazon S3 控制台：<https://console.aws.amazon.com/s3/>。
3. 选择您希望 AWS Config 用来传递配置项的存储桶，然后选择 Properties。
4. 选择 Permissions。
5. 选择 Edit Bucket Policy。
6. 将以下策略复制到 Bucket Policy Editor 窗口中：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "config.amazonaws.com"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName"
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "config.amazonaws.com"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/AWSLogs/sourceAccountID-WithoutHyphens/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```



```
}
```

7. 替换存储桶策略中的以下值：

- `targetBucketName` – AWS Config 将向其传递配置项的 Amazon S3 存储桶的名称。
- `[##] prefix` – Amazon S3 对象键的可选附加内容，可帮助在存储桶中创建类似文件夹的组织结构。
- `sourceAccountID-WithoutHyphens` – AWS Config 针对其向目标存储桶传递配置项的账户的 ID。

8. 选择 Save，然后选择 Close。

Amazon SNS 主题的权限

只有在您希望配置 AWS Config，传送另一账户拥有的 Amazon SNS 主题时，才使用此主题中的信息。

AWS Config 必须具有将通知发送到 SNS 主题的权限。如果您希望使用另一账户的 SNS 主题，请确保将以下策略附加至相应的 SNS 主题。

```
{
  "Id": "Policy1415489375392",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy20150201",
      "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` 为主题所有者的账号。对于 `account-id1`、`account-id2` 和 `account-id3`，请使用设置了 AWS Config 的账户的账号。

您必须用适当的值替换 `region` 和 `myTopic`。

AWS Config 的访问权限

当您授权 IAM 用户使用 AWS Config 控制台或 AWS CLI 的权限时，您可以（并且应该）将其权限限制到用户所需的最小范围内。

在大多数情况下，权限应涵盖以下常用操作：

- 设置和管理 AWS Config（完全访问权限）
- 使用 AWS Config（只读权限）

设置和管理 AWS Config 的用户必须具有完全访问权限。获得完全访问权限后，您可以执行关键的设置任务，例如：

- 提供 AWS Config 将数据传送到的 Amazon S3 和 Amazon SNS 终端节点
- 创建提供给 AWS Config 的角色
- 开启和关闭记录功能

使用 AWS Config 但无需进行设置的用户应该获得只读权限。对于查找资源配置或者按标签搜索资源的用户而言，这类权限非常有用。

授予 AWS Config 的只读权限

1. 通过 <https://console.aws.amazon.com/iam> 登录 AWS Identity and Access Management (IAM) 控制台。
2. 在导航窗格中，选择 Policies。
3. 在策略列表中，选择 AWSConfigUserAccess 策略。您可以使用 Filter 菜单和 Search 框来查找策略。
4. 选择 Policy Actions，然后选择 Attach。
5. 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。
6. 选择 Apply Policy。

授予 AWS Config 的完全访问权限

1. 通过 <https://console.aws.amazon.com/iam> 登录 AWS Identity and Access Management (IAM) 控制台。
2. 在导航窗格中选择 Policies，然后选择 Create Policy。
3. 对于 Create Your Own Policy，选择 Select。
4. 键入策略名称和描述。例如：AWSConfigFullAccess。
5. 对于 Policy Document，将完全访问策略键入或粘贴到编辑器中。您可以将 [完全访问权限示例 \(p. 134\)](#)。
6. 选择 Validate Policy 并确保屏幕顶部没有在红框中显示错误。更正报告的任何错误。
7. 选择 Create Policy 以保存新策略。
8. 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。
9. 选择 Policy Actions，然后选择 Attach。
10. 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。
11. 选择 Apply Policy。

Note

此外，您还可以从 IAM 控制台中创建内联策略并将其关联到 IAM 用户、组或角色，而不创建托管策略。有关更多信息，请参阅 IAM 用户指南 中的 [使用内联策略](#)。

示例策略

只读权限示例

以下 AWS 托管策略 (AWSConfigUserAccess) 可授予 AWS Config 的只读权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
    "config:Get*",
    "config:Describe*",
    "config:Deliver*",
    "config:List*",
    "tag:GetResources",
    "tag:GetTagKeys",
    "cloudtrail:DescribeTrails",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:LookupEvents"
  ],
  "Resource": "*"
}
]
```

完全访问权限示例

以下示例策略可授予 AWS Config 的完全访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sns:AddPermission",
        "sns:CreateTopic",
        "sns>DeleteTopic",
        "sns:GetTopicAttributes",
        "sns:ListPlatformApplications",
        "sns:ListTopics",
        "sns:SetTopicAttributes"
      ],
      "Resource": "arn:aws:sns:*"
    },
    {
      "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:PassRole",
        "iam:PutRolePolicy",
        "iam:AttachRolePolicy",

```

```
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeletePolicyVersion"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "config:*",
        "tag:Get*"
    ],
    "Resource": "*"
}
]
```

```
}
```

监控

您可以使用其他 AWS 服务来监控 AWS Config 资源。

- 每当用户通过 API 对支持的 AWS 资源进行创建、更新或修改时，您可以使用 Amazon Simple Notification Service (SNS) 向您发送通知。
- 您可以使用 Amazon CloudWatch Events 检测 AWS Config 事件状态的变更并对其进行响应。

主题

- [使用 Amazon SQS 监控 AWS 资源更改 \(p. 136\)](#)
- [使用 Amazon CloudWatch Events 监控 AWS Config \(p. 137\)](#)

使用 Amazon SQS 监控 AWS 资源更改

当用户通过 API 对支持的 AWS 资源进行创建、更新或修改时，AWS Config 会使用 Amazon Simple Notification Service (SNS) 向您发送通知。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。如果您想出于上述目的或其他目的以编程方式使用 AWS Config 的数据，请将 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[发送 Amazon SNS 信息至 Amazon SQS 队列](#)。

Amazon SQS 权限

要将 Amazon SQS 与 AWS Config 配合使用，您必须配置一项策略来为您的账户授予权限，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。在以下示例策略中，Amazon 资源名称 (ARN) 为 `arn:aws:sns:us-east-2:111122223333:test-topic` 的 SNS 主题可以对名为 `arn:aws:sqs:us-east-2:111122223333:test-topic-queue` 的主题执行任何操作。

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": "*",
      "Action": "sqs:*",
      "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 策略的特别信息](#)。

使用 Amazon CloudWatch Events 监控 AWS Config

Amazon CloudWatch Events 提供近乎实时的系统事件流以描述 AWS 资源变化。使用 Amazon CloudWatch Events 检测 AWS Config 事件状态的变更并对其进行响应。

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，Amazon CloudWatch Events 会根据您创建的规则，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 AWS Config 创建事件规则之前，您应当执行以下操作：

- 熟悉 CloudWatch Events 中的事件、规则和目标。有关更多信息，请参阅[什么是 Amazon CloudWatch Events ?](#)
- 有关如何开始使用 CloudWatch Events 并设置规则的信息，请参阅[CloudWatch Events 入门](#)。
- 创建将在您的事件规则中使用的目标。

主题

- [适用于 AWS Config 的 Amazon CloudWatch Events 格式 \(p. 138\)](#)
- [为 AWS Config 创建 Amazon CloudWatch Events 规则 \(p. 138\)](#)

适用于 AWS Config 的 Amazon CloudWatch Events 格式

适用于 AWS Config 的 CloudWatch 事件具有以下格式：

```
{
  "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}
}
```

为 AWS Config 创建 Amazon CloudWatch Events 规则

可以使用以下步骤创建对 AWS Config 发出的事件进行触发的 CloudWatch Events 规则。

1. 打开 CloudWatch 控制台 (<https://console.aws.amazon.com/cloudwatch/>)。
2. 在导航窗格中，选择 Events。
3. 选择 Create rule。
4. 在 Step 1: Create rule 页面上，对于 Service Name，选择 Config。
5. 对于 Event Type，选择用于触发此规则的事件类型：
 - 选择 All Events 以创建一个应用于所有 AWS 服务的规则。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 AWS API Call via 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 [使用 AWS CloudTrail 创建在 AWS API 调用上触发的 CloudWatch 事件规则](#)。
 - 选择 Config Configuration Item Change 以在您账户中的资源发生更改时获取通知。
 - 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。
 - 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。
6. 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：
 - 如果您选择 ConfigurationItemChangeNotification，则会在 AWS Config 成功将配置快照传送到您的 Amazon S3 存储桶时收到消息。
 - 如果您选择 ComplianceChangeNotification，则会在 AWS Config 评估的资源的合规性类型发生更改时收到消息。
 - 如果您选择 ConfigRulesEvaluationStarted，则会在 AWS Config 对照指定资源开始评估您的规则时收到消息。
 - 如果您选择 ConfigurationSnapshotDeliveryCompleted，则会在 AWS Config 成功将配置快照传送到您的 Amazon S3 存储桶时收到消息。
 - 如果您选择 ConfigurationSnapshotDeliveryFailed，则会在 AWS Config 无法将配置快照传送到您的 Amazon S3 存储桶时收到消息。
 - 如果您选择 ConfigurationSnapshotDeliveryStarted，则会在 AWS Config 开始将配置快照传送到您的 Amazon S3 存储桶时收到消息。

- 如果您选择 ConfigurationHistoryDeliveryCompleted，则会在 AWS Config 成功将配置历史记录传送到您的 Amazon S3 存储桶时收到消息。
7. 如果您从 Event Type 下拉列表中选择了某个特定事件类型，请选择 Any resource type 以创建一个应用于 AWS Config 支持的所有资源类型的规则。

或者，选择 Specific resource type(s)，然后键入 AWS Config 支持的资源类型 (例如，AWS::EC2::Instance)。
 8. 如果您从 Event Type 下拉列表中选择了某个特定事件类型，请选择 Any resource ID 以包括 AWS Config 支持的任何资源 ID。

或者，选择 Specific resource ID(s)，然后键入 AWS Config 支持的资源 ID (例如，i-04606de676e635647)。
 9. 如果您从 Event Type 下拉列表中选择了某个特定事件类型，请选择 Any rule name 以包括 AWS Config 支持的任何资源规则。

或者，选择 Specific rule name(s)，然后键入 AWS Config 支持的规则 (例如，required-tags)。
 10. 审查您的规则设置以确保其符合事件监控要求。
 11. 在 Targets 区域，选择 Add target*。
 12. 在 Select target type 列表中，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。
 13. 选择 Configure details。
 14. 在 Configure rule details 页面上，为规则键入名称和说明，然后选择 State 框以在创建规则后立即启用规则。
 15. 选择 Create rule 以确认您的选择。

使用 AWS CloudTrail 记录 AWS Config API 调用

AWS Config 已与 AWS CloudTrail 集成，后者是一种服务，可在 AWS 账户中捕获由 AWS 服务或代表其发出的 API 调用，并将日志文件传输到您指定的 Amazon Simple Storage Service 存储桶。CloudTrail 从 AWS Config 控制台或 AWS Config API 捕获所有 API 调用。通过 CloudTrail 收集的信息，您可以确定向 AWS Config 发出了什么请求、发出请求的源 IP 地址、何人发出的请求以及发出请求的时间等。要了解有关 CloudTrail 的更多信息，包括如何对其进行配置和启用，请参阅 [AWS CloudTrail User Guide](#)

CloudTrail 中的 AWS Config 信息

如果您在 AWS 账户中启用了 CloudTrail，它便会跟踪对 AWS Config 进行的 API 调用。AWS Config 记录会与其他 AWS 服务记录一起写入日志文件。CloudTrail 基于时间段和文件大小来确定何时创建新文件并向其写入内容。

所有 AWS Config 操作都会记录下来，[AWS Config API Reference](#) 中对这些操作进行了介绍。例如，对 [DeliverConfigSnapshot](#)、[DeleteDeliveryChannel](#) 和 [DescribeDeliveryChannels](#) 操作进行的调用会在 CloudTrail 日志文件中生成条目。

每个日志条目都包含有关生成请求的人员的信息。日志中的用户身份信息有助于确定发出的请求是否具有根或 IAM 用户证书，是否具有角色或联合用户的临时安全证书，或者是否是由其他 AWS 服务发出的。有关更多信息，请参阅 [CloudTrail 事件参考](#) 中的 `userIdentity` 字段。

默认情况下，将使用 Amazon S3 服务器端加密 (SSE) 对日志文件进行加密。日志文件可以在存储桶中存储任意长时间，不过您也可以定义 Amazon S3 生命周期规则以自动存档或删除日志文件。有关设置生命周期规则的信息，请参阅 Amazon Simple Storage Service 控制台用户指南 中的 [管理生命周期配置](#)。

如果您需要针对日志文件传输快速采取措施，可选择让 CloudTrail 在传输新的日志文件时发布 Amazon SNS 通知。有关更多信息，请参阅 [配置 Amazon SNS 通知](#)。

您还可以将多个 AWS 区域和多个 AWS 账户中的 AWS Config 日志文件聚合到单个 Amazon S3 存储桶中。更多信息，请参阅 [将 CloudTrail 日志文件聚合到单个 Amazon S3 存储桶中](#)。

了解 AWS Config 日志文件条目

CloudTrail 日志文件可包含一个或多个日志条目，每个条目由多个 JSON 格式的事件组成。一个日志条目表示来自任何源的一个请求，包括有关所请求的操作、任意参数以及操作的日期和时间等信息。日志条目不一定具有任何特定顺序。也即，它们不是公用 API 调用的有序堆栈跟踪。

示例日志文件

有关这些 CloudTrail 日志条目的类似示例，请参阅以下主题。

内容

- [DeleteDeliveryChannel](#) (p. 141)
- [DeliverConfigSnapshot](#) (p. 141)
- [DescribeConfigurationRecorderStatus](#) (p. 142)
- [DescribeConfigurationRecorders](#) (p. 142)

- [DescribeDeliveryChannels](#) (p. 143)
- [GetResourceConfigHistory](#) (p. 143)
- [PutConfigurationRecorder](#) (p. 144)
- [PutDeliveryChannel](#) (p. 145)
- [StartConfigurationRecorder](#) (p. 145)
- [StopConfigurationRecorder](#) (p. 146)

DeleteDeliveryChannel

下面是 [DeleteDeliveryChannel](#) 操作的一个 CloudTrail 日志文件示例。

```
{
  "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

下面是 [DeliverConfigSnapshot](#) 操作的一个 CloudTrail 日志文件示例。

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAABCDEFGHijklmnopq: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": "AIDAABCDEFGHijklmnopq",
        "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

下面是 [DescribeConfigurationRecorderStatus](#) 操作的一个 CloudTrail 日志文件示例。

```
{
    "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

下面是 [DescribeConfigurationRecorders](#) 操作的一个 CloudTrail 日志文件示例。

```
{
    "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

下面是 [DescribeDeliveryChannels](#) 操作的一个 CloudTrail 日志文件示例。

```
{
  "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

下面是 [GetResourceConfigHistory](#) 操作的一个 CloudTrail 日志文件示例。

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDAABCDEFHIJKLMNOPQ: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": "AIDAABCDEFGHijklmnopq",
        "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

下面是 [PutConfigurationRecorder](#) 操作的一个 CloudTrail 日志文件示例。

```
{
  "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

下面是 [PutDeliveryChannel](#) 操作的一个 CloudTrail 日志文件示例。

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::22222222222:user/JohnDoe",
    "accountId": "22222222222",
    "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-2:22222222222:config-api-test-pdx"
    }
  },
  "responseElements": null,
  "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
  "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
  "eventType": "AwsApiCall",
  "recipientAccountId": "22222222222"
}
```

StartConfigurationRecorder

下面是 [StartConfigurationRecorder](#) 操作的一个 CloudTrail 日志文件示例。

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::22222222222:user/JohnDoe",
    "accountId": "22222222222",
    "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": "22222222222"
}
```

```
}
```

StopConfigurationRecorder

下面是 [StopConfigurationRecorder](#) 操作的一个 CloudTrail 日志文件示例。

```
{
  "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"
}
```

AWS 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。

- [AWS Config](#) – 介绍 AWS Config 相关信息的主要网页。
- [AWS Config 定价](#)
- [技术方面常见问题](#)
- [合作伙伴](#) – 介绍合作伙伴的产品，这些产品与 AWS Config 充分集成，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 AWS 技能并获得实践经验。
- [AWS 开发人员工具](#) – 指向开发人员工具、软件开发工具包、IDE 工具包和命令行工具的链接，这些资源用于开发和管理 AWS 应用程序。
- [AWS 白皮书](#) – 指向 AWS 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 AWS 解决方案架构师或其他技术专家编写。
- [AWS Support 中心](#) - 用于创建和管理 AWS Support 案例的中心。还包括指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况和 AWS Trusted Advisor。
- [AWS Support](#) - 提供有关 AWS Support 信息的主要网页，是一种一对一的快速响应支持渠道，可帮助您在云中构建和运行应用程序。
- [联系我们](#) - 查询有关 AWS 账单、账户、事件、滥用和其他问题的中央联系点。
- [AWS 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 AWS Config 的 AWS 开发工具包

AWS 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 AWS 基础设施服务进行访问。AWS 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 AWS Config。

访问类型	说明
AWS 软件开发工具包	<p>AWS 提供以下软件开发工具包：</p> <ul style="list-style-type: none">• 适用于 C++ 文档的 AWS 开发工具包• AWS Mobile SDK for iOS 文档• 适用于 Go 文档的 AWS 开发工具包• AWS SDK for Java 文档• 适用于 JavaScript 文档的 AWS 开发工具包• 适用于 .NET 的 AWS 开发工具包 文档• 适用于 PHP 的 AWS 开发工具包文档• AWS SDK for Python (Boto) 文档• 适用于 Ruby 的 AWS 开发工具包 文档

访问类型	说明
第三方库	<p>AWS 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 AWS 开发人员中心获取这些资源：</p> <ul style="list-style-type: none">• AWS Java 开发人员中心• AWS JavaScript 开发人员中心• AWS PHP 开发人员中心• AWS Python 开发人员中心• AWS Ruby 开发人员中心• AWS Windows 和 .NET 开发人员中心

文档历史记录

下表介绍 AWS Config 的文档发布历史记录。

- API 版本：2014-11-12
- 最近一次更新文档的日期：2018 年 4 月 4 日

功能	描述	发行日期
AWS Config 支持新的托管规则	<p>此版本支持以下两新的托管规则：</p> <ul style="list-style-type: none"> • fms-webacl-resource-policy-check (p. 45) • fms-webacl-rulegroup-association-check (p. 45) <p>有关更多信息，请参阅 AWS 托管配置规则 (p. 28)。</p>	2018 年 4 月 4 日
多账户多区域数据聚合	<p>在此版本中，AWS Config 引入了多账户多区域数据聚合。此功能允许您将 AWS Config 数据从多个账户或一个组织和多个区域中聚合到一个聚合器账户。有关更多信息，请参阅 Multi-Account Multi-Region Data Aggregation (p. 107)。</p> <p>在此版本中，AWS Config 添加了以下新 API。有关更多信息，请参阅 AWS Config API 参考：</p> <ul style="list-style-type: none"> • PutConfigurationAggregator • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAuthorization • DescribeAggregationAuthorizations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRule • DescribeConfigurationAggregators • DescribeConfigurationAggregatorSourcesStatus • DeleteAggregationAuthorization • DeleteConfigurationAggregator 	2018 年 4 月 4 日
使用 Amazon CloudWatch Events 监控 AWS Config	<p>在此版本中，使用 Amazon CloudWatch Events 检测 AWS Config 事件状态的变更并对其进行响应。</p> <p>有关更多信息，请参阅 使用 Amazon CloudWatch Events 监控 AWS Config (p. 137)。</p>	2018 年 3 月 29 日

功能	描述	发行日期
新的 API 操作	在此版本中，AWS Config 添加了对 BatchGetResourceConfig API 的支持，使您可以批量检索一个或多个资源的当前状态。	2018 年 3 月 20 日
AWS Config 支持 AWS WAF RuleGroup 资源类型	在此版本中，您可以使用 AWS Config 记录将配置更改记录到 AWS WAF RuleGroup 和 AWS WAF RuleGroup 区域资源。 有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。	2018 年 2 月 15 日
AWS Config 支持新的托管规则	此版本支持以下 7 种新的托管规则： <ul style="list-style-type: none"> • elb-acm-certificate-required (p. 43) • elb-custom-security-policy-ssl-check (p. 43) • elb-predefined-security-policy-ssl-check (p. 44) • codebuild-project-envvar-awscred-check (p. 35) • codebuild-project-source-repo-url-check (p. 35) • iam-group-has-users-check (p. 47) • s3-bucket-server-side-encryption-enabled (p. 53) 有关更多信息，请参阅 AWS 托管配置规则 (p. 28)。	2018 年 1 月 25 日
AWS Config 支持 Elastic Load Balancing 资源类型	借助此版本，您可以使用 AWS Config 来记录对 Elastic Load Balancing Classic 负载均衡器所做的配置更改。 有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。	2017 年 11 月 17 日
AWS Config 支持 Amazon CloudFront 和 AWS WAF 资源类型	借助此版本，您可以使用 AWS Config 来记录对 CloudFront 分配和流分配所做的配置更改。 借助此版本，您可以使用 AWS Config 记录对以下 AWS WAF 和 AWS 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 AWS 资源类型 (p. 6)。	2017 年 11 月 15 日

功能	描述	发行日期
AWS Config 支持 AWS CodeBuild 资源类型	<p>借助此版本，您可以使用 AWS Config 记录对您的 AWS CodeBuild 项目所做的配置更改。</p> <p>有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。</p>	2017 年 10 月 20 日
AWS Config 支持 Auto Scaling 资源和一条新的托管规则	<p>借助此版本，您可以使用 AWS 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。</p> <p>有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。</p> <p>此版本还支持以下托管规则：</p> <ul style="list-style-type: none"> • autoscaling-group-elb-healthcheck-required (p. 31) <p>有关更多信息，请参阅 关于 AWS 托管 Config 规则 (p. 28)。</p>	2017 年 9 月 18 日
AWS Config 支持 AWS CodeBuild 资源类型	<p>借助此版本，您可以使用 AWS Config 记录对您的 AWS CodeBuild 项目所做的配置更改。</p> <p>有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。</p>	2017 年 10 月 20 日
AWS Config 支持 Auto Scaling 资源和一条新的托管规则	<p>借助此版本，您可以使用 AWS 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。</p> <p>有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。</p> <p>此版本还支持以下托管规则：</p> <ul style="list-style-type: none"> • autoscaling-group-elb-healthcheck-required (p. 31) <p>有关更多信息，请参阅 关于 AWS 托管 Config 规则 (p. 28)。</p>	2017 年 9 月 18 日

功能	描述	发行日期
AWS Config 支持 DynamoDB 表资源类型和一条新的托管规则	<p>借助此版本，您可以使用 AWS Config 记录对您的 DynamoDB 表所做的配置更改。</p> <p>有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。</p> <p>此版本支持以下托管规则：</p> <ul style="list-style-type: none"> • dynamodb-autoscaling-enabled (p. 37) <p>有关更多信息，请参阅 关于 AWS 托管 Config 规则 (p. 28)。</p>	2017 年 9 月 8 日
AWS Config 对 Amazon S3 支持两条新的托管规则	<p>此版本支持两条新的托管规则：</p> <ul style="list-style-type: none"> • s3-bucket-public-read-prohibited (p. 53) • s3-bucket-public-write-prohibited (p. 53) <p>有关更多信息，请参阅 关于 AWS 托管 Config 规则 (p. 28)。</p>	2017 年 8 月 14 日
AWS Config 控制台中的新页面	<p>您可以使用 AWS Config 控制台中的 Dashboard 来查看以下内容：</p> <ul style="list-style-type: none"> • 资源总数 • 规则总数 • 不合规资源数 • 不合规规则数 <p>有关更多信息，请参阅 查看 AWS Config 控制面板 (p. 24)。</p>	2017 年 7 月 17 日
新的 API 操作	<p>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 AWS Config 在您的 AWS 账户的区域中记录的资源总数。</p>	2017 年 7 月 17 日

功能	描述	发行日期
AWS Config 支持 AWS CloudFormation 堆栈资源类型和一条新的托管规则	<p>借助此版本，您可以使用 AWS Config 记录对您的 AWS CloudFormation 堆栈所做的配置更改。</p> <p>有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。</p> <p>此版本支持以下托管规则：</p> <ul style="list-style-type: none"> • cloudformation-stack-notification-check (p. 31) <p>有关更多信息，请参阅 关于 AWS 托管 Config 规则 (p. 28)。</p>	2017 年 6 月 7 日
新增和更新的内容	<p>此版本在加拿大 (中部) 区域和南美洲 (圣保罗) 区域中增加了对 AWS Config 规则的支持。</p> <p>有关支持 AWS Config 和 Config Rules 的所有区域，请参阅 AWS General Reference 中的 AWS 区域和终端节点。</p>	2017 年 5 月 7 日
新增和更新的内容	<p>AWS Config 规则在 AWS GovCloud (US) 区域中可用。有关更多信息，请参阅 AWS GovCloud (US) User Guide。</p> <p>有关支持 AWS Config 的区域，请参阅 AWS General Reference 中的 AWS 区域和终端节点。</p>	2017 年 6 月 8 日
AWS Config 支持 Amazon CloudWatch 警报资源类型和三个新托管规则	<p>借助此版本，您可以使用 AWS Config 记录您的 Amazon CloudWatch 警报的配置更改。</p> <p>有关更多信息，请参阅 支持的 AWS 资源类型 (p. 6)。</p> <p>此版本支持三条新的托管规则：</p> <ul style="list-style-type: none"> • cloudwatch-alarm-action-check (p. 33) • cloudwatch-alarm-resource-check (p. 34) • cloudwatch-alarm-settings-check (p. 34) <p>有关更多信息，请参阅 关于 AWS 托管 Config 规则 (p. 28)。</p>	2017 年 6 月 1 日

功能	描述	发行日期
新增和更新的内容	<p>此版本支持为以下托管规则指定应用程序版本号：</p> <ul style="list-style-type: none"> • ec2-managedinstance-applications-blacklisted (p. 40) • ec2-managedinstance-applications-required (p. 40) <p>有关更多信息，请参阅 关于 AWS 托管 Config 规则 (p. 28)。</p>	2017 年 6 月 1 日
新增和更新的内容	<p>此版本在亚太地区（孟买）区域中增加了对 AWS Config 规则的支持。有关更多信息，请参阅 AWS General Reference 中的 AWS 区域和终端节点。</p>	2017 年 27 月 4 日
新增和更新的内容	<p>此版本支持更新的控制台体验，可让您首次将 AWS Config 托管规则添加到您的账户。</p> <p>当您首次设置 AWS Config 规则或者在新区域中设置这些规则时，您可以按名称、说明或标签搜索 AWS 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。</p> <p>有关更多信息，请参阅 使用控制台设置 AWS Config (p. 17)。</p>	2017 年 4 月 5 日
AWS Config 支持新的托管规则	<p>此版本支持以下 7 种新的托管规则：</p> <ul style="list-style-type: none"> • acm-certificate-expiration-check (p. 30) • ec2-instance-detailed-monitoring-enabled (p. 39) • ec2-managedinstance-inventory-blacklisted (p. 41) • ec2-volume-inuse-check (p. 42) • iam-user-group-membership-check (p. 47) • iam-user-no-policies-check (p. 48) • s3-bucket-ssl-requests-only (p. 54) <p>有关更多信息，请参阅 AWS 托管配置规则 (p. 28)。</p>	2017 年 2 月 21 日
新增和更新的内容	<p>此版本在欧洲（伦敦）区域中增加了对 AWS Config 规则的支持。有关更多信息，请参阅 AWS General Reference 中的 AWS 区域和终端节点。</p>	2017 年 2 月 21 日

功能	描述	发行日期
新增和更新的内容	此版本增加了适用于 AWS Config 托管规则的 AWS 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 AWS CloudFormation 模板创建 AWS Config 托管规则 (p. 56) 。	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 AWS Lambda 函数是否将评估结果传送到 AWS Config。不会更新现有评估，并且不会将评估结果发送到 AWS Config。 有关更多信息，请参阅 AWS Config API Reference 中的 PutEvaluations。	2017 年 2 月 16 日
新增和更新的内容	此版本在亚太区域（首尔）和美国西部（加利福尼亚北部）区域中增加了对 AWS Config 规则的支持。有关更多信息，请参阅 AWS General Reference 中的 AWS 区域和终端节点 。	2016 年 12 月 21 日
新增和更新的内容	此版本在 欧洲（伦敦）区域 中增加了对 AWS Config 的支持。有关更多信息，请参阅 AWS General Reference 中的 AWS 区域和终端节点 。	2016 年 12 月 13 日
新增和更新的内容	此版本在 加拿大（中部）区域 中增加了对 AWS Config 的支持。有关更多信息，请参阅 AWS General Reference 中的 AWS 区域和终端节点 。	2016 年 12 月 8 日
AWS Config 支持 Amazon Redshift 资源类型和两条新的托管规则	在此版本中，您可以使用 AWS Config 记录您的 Amazon Redshift 群集、群集参数组、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、配置项和关系 (p. 6) 。 此版本支持两条新的托管规则： <ul style="list-style-type: none">• redshift-cluster-configuration-check (p. 49)• redshift-cluster-maintenancesettings-check (p. 50) 有关更多信息，请参阅 AWS 托管配置规则 (p. 28) 。	2016 年 12 月 7 日

功能	描述	发行日期
新增和更新的内容	<p>此版本增加了对新托管规则的支持：</p> <ul style="list-style-type: none"> • dynamodb-throughput-limit-check (p. 38) <p>有关更多信息，请参阅 AWS 托管配置规则 (p. 28)。</p>	2016 年 12 月 7 日
新增和更新的内容	<p>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 AWS General Reference 中的 AWS Config 限制。</p>	2016 年 12 月 7 日
AWS 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。	<p>您可以使用此版本的 AWS Config 记录托管实例的软件配置变更，还支持托管实例清单。</p> <p>有关更多信息，请参阅 记录托管实例的软件配置 (p. 8)。</p> <p>此版本支持三条新的托管规则：</p> <ul style="list-style-type: none"> • ec2-managedinstance-inventory-blacklisted (p. 41) • ec2-managedinstance-applications-required (p. 40) • ec2-managedinstance-platform-check (p. 41) <p>有关更多信息，请参阅 AWS 托管配置规则 (p. 28)。</p>	2016 年 12 月 1 日
AWS Config 支持 Amazon S3 存储桶资源和两条新的托管规则	<p>借助此版本，您可以使用 AWS Config 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、配置项和关系 (p. 6)。</p> <p>此版本支持两条新的托管规则：</p> <ul style="list-style-type: none"> • s3-bucket-logging-enabled (p. 52) • s3-bucket-versioning-enabled (p. 54) <p>有关更多信息，请参阅 关于 AWS 托管 Config 规则 (p. 28)。</p>	2016 年 10 月 18 日
新增和更新的内容	<p>此版本在美国东部（俄亥俄）区域中增加了对 AWS Config 和 AWS Config 规则的支持。有关更多信息，请参阅 AWS General Reference 中的 AWS 区域和终端节点。</p>	2016 年 10 月 17 日

功能	描述	发行日期
新增和更新的管理规则	<p>此更新添加了对八个新的管理规则的支持：</p> <ul style="list-style-type: none"> • approved-amis-by-id (p. 30) • approved-amis-by-tag (p. 31) • db-instance-backup-enabled (p. 36) • desired-instance-type (p. 37) • ebs-optimized-instance (p. 39) • iam-password-policy (p. 46) • rds-multi-az-support (p. 48) • rds-storage-encrypted (p. 49) <p>您可以为以下规则指定多个参数值：</p> <ul style="list-style-type: none"> • desired-instance-tenancy (p. 36) • required-tags (p. 50) <p>有关更多信息，请参阅 AWS 托管配置规则 (p. 28)。</p>	2016 年 10 月 4 日
AWS Config 控制台的新增和更新内容	<p>此更新增加了支持，用以在 AWS Config 时间线中查看 AWS CloudTrail API 活动。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 在 AWS Config 控制台中查看配置详细信息 (p. 79)。</p>	2016 年 9 月 6 日
AWS Config 支持 Elastic Load Balancing 资源类型	<p>借助此版本，您可以使用 AWS Config 来记录 Elastic Load Balancing 应用程序负载均衡器的配置更改。有关更多信息，请参阅 支持的资源、配置项和关系 (p. 6)。</p>	2016 年 8 月 31 日
新增和更新的内容	<p>此版本在亚太区域（新加坡）和亚太区域（悉尼）区域中增加了对 AWS Config 规则的支持。有关更多信息，请参阅 AWS General Reference 中的 AWS 区域和终端节点。</p>	2016 年 8 月 18 日
AWS Config 规则的新增和更新内容	<p>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 AWS Config 规则指定触发器 (p. 26)。</p> <p>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 手动评估您的资源 (p. 76)。</p> <p>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. 61)。</p>	2016 年 7 月 25 日

功能	描述	发行日期
AWS Config 支持 Amazon RDS 和 AWS Certificate Manager (ACM) 资源类型	借助此版本，您可以使用 AWS Config 来记录您的 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 AWS Config 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、配置项和关系 (p. 6) 。	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. 122) 的配置记录器。	2016 年 7 月 07 日
简化的角色创建过程和更新策略	通过此更新，为 AWS Config 创建 IAM 角色的过程得到了简化。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 AWS Config (p. 15) 中的步骤、 针对 Amazon S3 存储桶的权限 (p. 130) 中的示例策略及 AWS Config 的访问权限 (p. 132) 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 AWS Config 规则 (Node.js) 的示例 AWS Lambda 函数 (p. 62) 中提供了更新的示例函数，并在 AWS Config 规则的示例事件 (p. 67) 中添加了示例事件。	2016 年 3 月 29 日
AWS Config Rules 的 GitHub 存储库	此更新将关于 AWS Config 规则 GitHub 存储库 的信息添加到 使用 AWS Config 规则评估资源 (p. 26) 中。此存储库提供了 AWS 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
AWS Config 规则	此版本介绍了 AWS Config 规则。借助规则，您可以使用 AWS Config 评估您的 AWS 资源是否符合您所需的配置。有关更多信息，请参阅 使用 AWS Config 规则评估资源 (p. 26) 。	2015 年 12 月 18 日
AWS Config 支持 IAM 资源类型	借助此版本，您可以使用 AWS Config 记录您的 IAM 用户、组、角色和客户托管策略的配置更改。有关更多信息，请参阅 支持的资源、配置项和关系 (p. 6) 。	2015 年 12 月 10 日
AWS Config 支持 EC2 专用主机	借助此版本，您可以使用 AWS 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、配置项和关系 (p. 6) 。	2015 年 11 月 23 日

功能	描述	发行日期
更新的权限信息	<p>此更新添加了关于 AWS Config 的下列 AWS 托管策略的信息：</p> <ul style="list-style-type: none"> • <code>AWSConfigRole</code> – 授予 AWS Config 获取您的资源的配置详细信息的权限。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. 129)。 • <code>AWSConfigUserAccess</code> – 授予 AWS Config 用户只读权限。有关更多信息，请参阅 AWS Config 的访问权限 (p. 132)。 	2015 年 10 月 19 日
AWS Config 规则预览	<p>此版本介绍了 AWS Config 规则预览。借助规则，您可以使用 AWS Config 评估您的 AWS 资源是否符合您所需的配置。有关更多信息，请参阅 使用 AWS Config 规则评估资源 (p. 26)。</p>	2015 年 10 月 7 日
新增和更新的内容	<p>此版本增加了查找 AWS Config 发现的资源的功能。有关更多信息，请参阅 查找 AWS Config 发现的资源 (p. 78)。</p>	2015 年 8 月 27 日
新增和更新的内容	<p>此版本增加了选择 AWS Config 记录哪些类型资源的功能。有关更多信息，请参阅 选择 AWS Config 所记录的资源 (p. 124)。</p>	2015 年 6 月 23 日
新增和更新的内容	<p>此版本增加了对下列区域的支持：亚太区域（东京）、亚太区域（新加坡）、欧洲（法兰克福）、南美洲（圣保罗）和美国西部（加利福尼亚北部）。有关更多信息，请参阅 AWS 区域和终端节点。</p>	2015 年 4 月 6 日
新增和更新的内容	<p>此版本新增了创建对 Amazon SNS 主题的电子邮件订阅（可选）的支持。您也可以使用电子邮件筛选条件监控特定的资源更改。有关更多信息，请参阅 通过电子邮件监控 AWS Config 资源变更 (p. 90)。</p>	2015 年 3 月 27 日
新增和更新的内容	<p>此版本支持与 AWS CloudTrail 集成，以记录所有的 AWS Config API 活动。有关更多信息，请参阅 使用 AWS CloudTrail 记录 AWS Config API 调用 (p. 140)。</p> <p>此版本新增了对下列区域的支持：美国西部（俄勒冈）、欧洲（爱尔兰）和亚太区域（悉尼）。</p> <p>此版本还包括下列文档更新：</p> <ul style="list-style-type: none"> • 关于监控 AWS Config 配置的信息 • 文档的各种修订 	2015 年 2 月 10 日
新指南	<p>此版本介绍了 AWS Config。</p>	2014 年 11 月 12 日

AWS 词汇表

有关最新 AWS 术语，请参阅 AWS General Reference 中的 [AWS 词汇表](#)。