亚马逊云科技

开发人员指南

Amazon Config

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

Amazon Config: 开发人员指南

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

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

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

Table of Contents

什么是 Amazon Config？ 1
注意事项 1
Amazon Config 的使用方式 1
资源管理 1
审计与合规性 2
对配置更改进行管理与故障排除 2
安全分析 2
合作伙伴解决方案 2
特征 2
Amazon Config工作原理 3
资源发现 4
资源跟踪 4
配置项的交付 5
控制对的访问权限Amazon Config 7
术语和概念 8
Amazon Config 接口 9
资源管理 9
配置记录器 10
传输通道 5
Amazon Config 规则 11
Amazon服务集成 14
Amazon Organizations 14
Amazon Control Tower 14
Amazon CloudTrail 14
Amazon Security Hub CSPM 15
Amazon Trusted Advisor 15
Amazon Audit Manager 16
Amazon Systems Manager 16
Amazon Firewall Manager 16
Amazon EC2 专用主机 16
应用程序负载均衡器 17
Amazon CodeBuild 17
Amazon X-Ray 17
Amazon 服务管理连接器 17

Amazon API Gateway 17
区域支持 18
注意事项 18
受支持区域列表 18
服务限制 22
补充信息 24
Amazon适用于 的 软件开发工具包Amazon Config 25
开始使用 26
报名参加Amazon 26
注册获取Amazon Web Services 账户 26
保护 IAM 用户 26
入门方法Amazon Config 27
设置 （控制台） 27
设置 27
一键设置 28
手动设置 31
设置（Amazon CLI） 37
设置 37
先决条件 37
启动 Amazon Config 104
验证设置 107
与Amazon SDKs 109
配置记录器 111
客户管理的配置记录器的注意事项 111
服务相关配置记录器的注意事项 112
受支持的服务 114
配置记录器的偏离检测 114
启动客户管理的配置记录器 115
停止客户管理的配置记录器 115
更改客户管理的配置记录器的记录频率 116
重命名客户管理的配置记录器 119
查看配置记录器 119
删除配置记录器 121
传输通道 122
注意事项 122
术语 123

配置项的组成部分 123
查看传输通道 125
更新传递通道 126
重命名传递通道 130
传送配置快照 132
传送配置快照 132
验证传送状态 132
查看配置快照 133
查看配置快照 133
配置快照示例 134
示例通知 139
示例配置项变更通知 140
示例配置历史记录传输通知 153
示例配置快照传输开始通知 154
示例配置快照传输通知 154
示例合规性变更通知 155
示例规则评估开始通知 159
示例过大配置项变更通知 160
示例传输失败通知 162
Amazon Config 控制面板 164
合规性和资源清单 164
Amazon Config 使用情况和成功指标 165
资源管理 168
支持的资源类型 168
Amazon AppStream 170
Amazon AppFlow 170
Amazon AppIntegrations 170
Amazon API Gateway 171
Amazon Athena 172
Amazon Bedrock 172
Amazon CloudFront 173
Amazon CloudWatch 174
Amazon CodeGuru 175
Amazon Cognito 176
Amazon Comprehend 176
Amazon Connect 176

Amazon Detective 177
Amazon DynamoDB 178
Amazon EC2 178
Amazon ECR 187
Amazon ECS 188
Amazon EFS 189
Amazon EKS 189
Amazon EMR 190
Amazon EMR Serverless 190
Amazon EventBridge 190
Amazon Forecast 191
Amazon Fraud Detector 192
Amazon GameLift 192
Amazon GuardDuty 193
Amazon Inspector 193
Amazon IVS 194
Amazon Keyspaces 194
Amazon Location Service 194
亚马逊 OpenSearch 服务 195
Amazon Personalize 196
Amazon Pinpoint 196
Amazon QLDB 197
Amazon Kendra 198
Amazon Kinesis 198
Amazon Lex 199
Amazon Lightsail 199
Amazon Lookout for Metrics 199
Amazon Lookout for Vision 200
Amazon Macie 200
Amazon Managed Grafana 200
Amazon Managed Service for Prometheus 200
Amazon MemoryDB 201
Amazon MQ 201
Amazon MSK 201
Amazon Quick Suite 202
Amazon Redshift 202

Amazon RDS 204
Amazon Route 53 205
亚马逊 SageMaker AI 207
Amazon SES 210
Amazon SNS 210
Amazon SQS 211
Amazon S3 211
Amazon WorkSpaces 213
Amazon Amplify 214
Amazon AppConfig 214
Amazon App Runner 215
Amazon App Mesh 215
Amazon AppSync 216
Amazon Audit Manager 216
Amazon Auto Scaling 217
Amazon B2B 数据交换 217
Amazon Backup 218
Amazon Batch 219
Amazon 账单与成本管理 219
Amazon Budgets 219
Amazon Certificate Manager 220
Amazon 干净的房间 220
Amazon CloudFormation 220
Amazon CloudTrail 221
Amazon Cloud9 221
Amazon Cloud Map 222
Amazon CodeArtifact 222
Amazon CodeBuild 223
Amazon CodeDeploy 223
Amazon CodePipeline 224
Amazon Config 224
Amazon DMS 225
Amazon DataSync 226
Amazon 截止日期云 227
Amazon Device Farm 228
Amazon Elastic Beanstalk 228

Amazon Entity Resolution 数据匹配服务 229
Amazon FIS 230
Amazon Global Accelerator 230
Amazon Glue 230
Amazon Ground Station 231
Amazon HealthLake 232
Amazon IAM 232
Amazon IoT 233
Amazon KMS 237
Amazon Lambda 238
Amazon Mainframe Modernization 238
Amazon Network Firewall 238
Amazon Network Manager 239
Amazon 组织 241
Amazon Panorama 241
Amazon 私有 CA 241
Amazon Resilience Hub 242
Amazon 资源探索器 242
Amazon RoboMaker 242
Amazon Signer 243
Amazon Secrets Manager 243
Amazon Security Hub CSPM 244
Amazon Service Catalog 244
Amazon Shield 245
Amazon Step Functions 245
Amazon Systems Manager 246
Amazon Transfer Family 247
Amazon WAF 247
Amazon X-Ray 249
Elastic Load Balancing 249
MediaConnect 251
MediaPackage 251
MediaPackage 252
MediaTailor 252
按区域可用性列出的资源覆盖范围 253
北美洲和南美洲 253

欧洲 309
亚太地区 356
中国 423
非洲和中东 446
GovCloud 480
记录 Amazon 资源 507
注意事项 508
区域性资源和全局资源 508
Amazon Config 规则和全局资源类型 512
记录频率 513
未记录的资源 513
记录资源（控制台） 514
记录资源（Amazon CLI） 517
排除资源 525
停止记录 525
记录第三方资源（Amazon CLI） 525
添加资源 526
记录配置项 529
读取配置项 530
删除资源 531
记录软件配置 532
先决条件 532
记录软件配置 533
查找资源 534
查看资源 535
查看合规性（控制台） 536
查看合规性 (Amazon SDKs) 536
查看合规性历史记录 544
查看合规性历史记录（控制台） 544
查看合规性历史记录（Amazon CLI） 544
对于资源和规则 550
查询合规性历史记录 551
为资源添加标签 552
与标记相关的限制 553
使用 Amazon Config API 操作管理标签 553
Amazon Config 规则 554

注意事项 554
区域支持 556
规则的组成部分 563
Amazon Config 规则是如何运作的 564
触发器类型 564
评估模式 565
规则元数据 566
托管规则 567
托管规则的列表 568
按评估模式划分的托管规则列表 740
按触发器类型划分的托管规则列表 765
按区域可用性列出的托管规则列表 789
使用 Amazon CloudFormation 模板创建托管规则 1403
自定义规则 1405
自定义策略规则 1405
自定义 Lambda 规则 1405
Amazon Config 自定义规则的格式差异 1405
创建自定义策略规则 1406
创建自定义 Lambda 规则 1412
管理自定义 Lambda 规则的已删除资源 1433
服务相关规则 1434
添加规则 1435
使用控制台 1435
使用 Amazon SDKs 1438
更新规则 1442
使用控制台 1442
使用 Amazon SDKs 1443
删除规则 1447
注意事项 1448
使用控制台 1448
使用 Amazon SDKs 1449
查看规则 1451
使用控制台 1451
使用 Amazon SDKs 1452
开启主动评估 1464
使用控制台 1464

使用 Amazon SDK 1466
向 Security Hub CSPM 发送评估 1470
向 Security Hub CSPM 发送规则评估 1470
使用规则评估资源 1470
删除评估结果 1474
问题排查 1475
修复 1478
区域支持 1478
设置手动修正 1481
设置自动修正 1483
删除修正操作 1484
聚合器 1486
应用场景 1486
术语 1487
区域支持 1487
聚合器控制面板 1491
使用聚合器控制面板 1491
合规性控制面板 1493
清单控制面板 1495
创建聚合器 1497
注册委托管理员 1501
编辑聚合器 1503
删除聚合器 1505
授权聚合器账户 1506
注意事项 1506
添加授权 1506
删除授权 1508
注意事项 1508
删除授权 1509
查看聚合器 1509
故障排除 1511
高级查询 1513
功能 1513
查询组件 1514
摘要 1514
参数 1514

示例 1515
查询编辑器（控制台） 1515
注意事项 1515
使用 Amazon 示例查询 1516
创建您的自定义查询 1516
查询编辑器（Amazon CLI） 1517
注意事项 1517
查询资源配置数据 1518
保存查询 1519
查看所有已保存的查询 1520
获取已保存的查询的详细信息 1521
删除已保存的查询 1521
自然语言查询处理器 1522
注意事项 1522
使用自然语言查询处理器进行查询 1516
提示示例 1523
提供反馈 1527
区域支持 1527
示例查询 1528
关系查询示例 1533
限制 1535
CIDR 范围 notation/IP 1537
一个数组中有多个属性 1537
区域支持 1538
删除数据 1543
设置数据保留期（控制台） 1545
安全性 1546
数据保护 1546
传输中的数据的加密 1547
传输中的数据的加密 1547
身份和访问管理 1547
受众 1548
使用身份进行身份验证 1548
使用策略管理访问 1549
如何 Amazon Config 与 IAM 配合使用 1550
基于身份的策略示例 1555

Amazon 托管策略 1572
IAM 角色的权限 1747
更新 IAM 角色 1751
Amazon S3 存储桶的权限 1752
KMS 密钥的权限 1756
Amazon SNS 主题的权限 1759
问题排查 1762
使用服务相关角色 1764
事件响应 1765
合规性验证 1766
恢复能力 1766
基础设施安全性 1766
配置和漏洞分析 1767
防止跨服务混淆代理 1767
最佳实践 1768
日志记录和监控 1769
日志记录 1769
Amazon Config中的信息 CloudTrail 1769
了解Amazon Config日志文件条目 1770
示例日志文件 1770
监控 1778
使用 Amazon SQS 1778
使用 Amazon EventBridge 1780
Amazon VPC 端点 1787
创建 VPC 终端节点 1787
常见问题解答 1788
看不到我最新的配置更改 1788
我可以立即查看我的配置更改吗？ 1788
Amazon Config 中的间接关系 1788
什么是资源关系？ 1788
什么是与资源的直接关系和间接关系？ 1789
Amazon Config 支持哪些间接关系？ 1789
哪些场景使用间接关系？ 1791
由于直接关系和间接关系，配置项是如何创建的？ 1792
由于间接关系而生成的配置项有哪些？ 1792
如何禁用间接关系？ 1794

如何检索与间接关系相关的配置数据？ 1794
代码示例 1796
基本功能 1796
操作 1797
文档历史记录 1834
早期更新 1964
..... mmx

什么是 Amazon Config？

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

Amazon 资源是您可以在 Amazon 中使用的实体，例如 Amazon Elastic Compute Cloud（EC2）实例、Amazon Elastic Block Store（EBS）卷、安全组或 Amazon 虚拟私有云（VPC）。有关 Amazon 支持的 Amazon Config 资源的完整列表，请参阅 支持的资源类型 Amazon Config

注意事项

- Amazon Web Services 账户：您需要一个活跃。Amazon Web Services 账户有关更多信息，请参阅注册。Amazon
- Amazon S3 存储桶：您需要一个 S3 存储桶才能接收配置快照和历史记录的数据。有关更多信息，请参阅 Amazon S3 存储桶的权限。
- Amazon SNS 主题：当您的配置快照和历史记录发生变化时，您需要 Amazon SNS 才能收到通知。有关更多信息，请参阅 Amazon SNS 主题的权限。
- IAM 角色：您需要一个 IAM 角色，该角色有权访问。Amazon Config有关更多信息，请参阅 IAM 角色的权限。
- 资源类型：您可以决定希望 Amazon Config 记录哪些资源类型。有关更多信息，请参阅记录 Amazon 资源。

Amazon Config 的使用方式

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

资源管理

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

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

审计与合规性

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

对配置更改进行管理与故障排除

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

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

安全分析

要分析潜在的安全漏洞，您需要了解有关您的 Amazon 资源配置的详细历史记录信息，例如向您的用户授予的 Amazon Identity and Access Management（IAM）权限或者控制对资源的访问的 Amazon EC2 安全组规则。

您可以使用 Amazon Config 随时查看 Amazon Config 正在记录的分配给用户、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 日是否拥有修改 Amazon VPC 设置的权限。

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

合作伙伴解决方案

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

特征

在您设置 Amazon Config 时，可以完成以下操作：

资源管理

- 指定您希望 Amazon Config 记录的资源类型。

- 设置 Amazon S3 桶以接收配置快照（按需）和配置历史记录。
- 设置 Amazon SNS 以发送配置流通知。
- 向 Amazon Config 授予访问 Amazon S3 存储桶和 Amazon SNS 主题所需的权限。

  有关更多信息，请参阅查看 Amazon 资源配置和历史记录以及管理 Amazon 资源配置和历史记录。

规则和合规包

- 指定您希望 Amazon Config 评估所记录资源类型的合规性信息使用的规则。
- 使用合规包或一系列规则，这些规则可作为 Amazon Web Services 账户中的单个实体进行部署和监控。

  有关更多信息，请参阅使用 Amazon Config 规则评估资源和合规包。

补救措施：

- 修复由 Amazon Config 规则 评估的不合规资源。

  有关更多信息，请参阅修正。

聚合器

- 使用聚合器集中查看您的资源清单和合规性。聚合器会将多个 Amazon Web Services 账户和 Amazon 区域中的 Amazon Config 配置和合规性数据收集到一个账户和区域中。

  有关更多信息，请参阅多账户多区域数据聚合。

高级查询

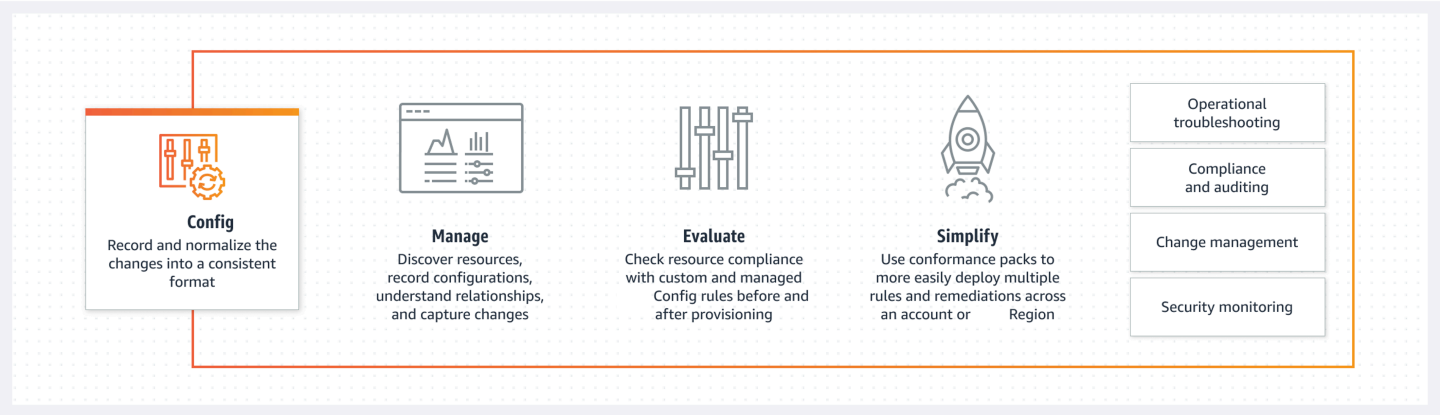
- 使用其中一个示例查询，或者参考 Amazon 资源的配置架构编写自己的查询。

  有关更多信息，请参阅查询 Amazon 资源的当前配置状态。

Amazon Config工作原理

Amazon Config提供了您Amazon账户中Amazon资源配置的详细视图。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。

Amazon资源是您可以在其中使用的实体Amazon，例如亚马逊弹性计算云 (EC2) 实例、亚马逊弹性区块存储 (EBS) 卷、安全组或亚马逊虚拟私有云 (VPC)。有关支持的Amazon资源的完整列表Amazon Config，请参阅支持的资源类型 Amazon Config。



资源发现

开启后Amazon Config，它会首先发现您账户中存在的受支持Amazon资源，然后为每种资源生成一个配置项目。

Amazon Config当资源配置发生变化时，它还会生成配置项目，并且它会维护自启动配置记录器之时起的资源配置项目的历史记录。默认情况下，Amazon Config会为该区域中所有支持的资源创建配置项目。如果您不Amazon Config想为所有支持的资源创建配置项目，则可以指定希望它跟踪的资源类型。

在指定Amazon Config要跟踪的资源类型之前，请检查按区域可用性划分的资源覆盖率，以查看您设置的Amazon区域是否支持该资源类型Amazon Config。如果至少有一个区域支持某种资源类型，则即使您正在设置的区域不支持指定的资源类型Amazon Config，您也可以在支持的所有Amazon区域中启用该资源类型的记录Amazon Config。Amazon Config

资源跟踪

Amazon Config通过对账户中的每个资源调用 Describe 或 List API 调用，跟踪资源的所有更改。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 安全组中移除出口规则会导致Amazon Config在该安全组上调用 Describe API 调用。Amazon Config然后在与安全组关联的所有实例上调用 Describe API 调用。安全组（资源）以及每个实例（相关资源）的更新后配置将被记录为配置项，并以配置流的形式传送到 Amazon Simple Storage Service（Amazon S3）存储桶。

Amazon Config还会跟踪不是由 API 启动的配置更改。Amazon Config定期检查资源配置，并为已更改的配置生成配置项目。

如果您使用的是Amazon Config规则，请Amazon Config持续评估您的Amazon资源配置以确定所需的设置。根据规则，Amazon Config将根据配置更改或定期评估您的资源。每个规则都与一个Amazon Lambda函数关联，其中包含规则的评估逻辑。在Amazon Config评估您的资源时，它会调用规则的函数。Amazon Lambda该函数会返回被评估资源的合规性状态。如果资源违反了规则的条件，则会将该资源和规则Amazon Config标记为不合规。当资源的合规状态发生变化时，Amazon Config会向您的 Amazon SNS 主题发送通知。

配置项的交付

Amazon Config可以通过以下渠道之一交付配置项目：

Amazon S3 存储桶

Amazon Config跟踪Amazon资源配置的变化，并定期将更新的配置详细信息发送到您指定的 Amazon S3 存储桶。对于每种Amazon Config记录的资源类型，它每六小时发送一次配置历史记录文件。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。每个文件都包含一种类型的资源，例如 Amazon EC2 实例或 Amazon EBS 卷。如果没有发生配置更改，则Amazon Config不发送文件。

Amazon Config当您在 CLI 中使用deliver-config-snapshot命令或在Amazon Config AP Amazon I 中使用DeliverConfigSnapshot操作时，会将配置快照发送到您的 Amazon S3 存储桶。配置快照包含Amazon Config在您的Amazon Web Services 账户中记录的所有资源的配置详细信息。配置历史记录文件和配置快照均采用 JSON 格式。

> **Note**
>
> Amazon Config仅将配置历史文件和配置快照传送到指定的 S3 存储桶；Amazon Config不会修改 S3 存储桶中对象的生命周期策略。您可以使用生命周期策略指定是删除对象，还是将对象存档到 Amazon Glacier。有关更多信息，请参阅《Amazon Simple Storage Service 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）主题是一个沟通渠道，Amazon SNS 使用它将消息（或通知）传送到订阅端点，例如电子邮箱地址或客户端。其他类型的 Amazon SNS 通知包括传送到手机应用程序上的推送通知消息、传送到支持短信服务功能的手机上的短信服务（SMS）通知以

及 HTTP POST 请求。为了获得最佳效果，请使用 SQS 作为 SNS 主题的通知端点，然后以编程方式处理通知中的信息。

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

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

通知可以是以下任一类型的消息。

消息类型	描述
ComplianceChangeNotification	Amazon Config评估的资源的合规性类型已更改。合规性类型表示资源是否符合特定Amazon Config规则，它由消息中的`ComplianceType` 密钥表示。消息中包含 `newEvaluationResult` 和 `oldEvaluationResult` 对象，以便进行比较。
ConfigRulesEvaluationStarted	Amazon Config已开始根据指定资源评估您的规则。
ConfigurationSnapshotDeliveryStarted	Amazon Config已开始将配置快照传送到您的 Amazon S3 存储桶。Amazon S3 存储桶的名称是为消息中的 `s3Bucket` 键提供的。
ConfigurationSnapshotDeliveryCompleted	Amazon Config已成功将配置快照传送到您的 Amazon S3 存储桶。
ConfigurationSnapshotDeliveryFailed	Amazon Config未能将配置快照传送到您的 Amazon S3 存储桶。
ConfigurationHistoryDeliveryCompleted	Amazon 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。此消息包括为此更改Amazon Config创建的配置项目的详细信息，还包括更改的类型。上述通知均在发生更改后的几分钟内传送，统称为配置流。

消息类型	描述
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。除短信外，Amazon SNS 消息最多可以包含 256 KB 的文本数据，包括 XML、JSON 和未格式化的文本。您可以在指定的 Amazon S3 存储桶位置查看完整通知。
OversizedConfigurationItemChangeDeliveryFailed	Amazon Config未能将超大配置项目变更通知传送到您的 Amazon S3 存储桶。

有关示例通知，请参阅 Amazon Config 发送到 Amazon SNS 主题的通知 有关 Amazon SNS 的更多信息，请参阅 Amazon Simple Notification Service 开发人员指南。

> **Note**
>
> 为什么我看不到我最新的配置更改？
> Amazon Config通常会在检测到更改后立即或按您指定的频率记录对资源的配置更改。但是，这需要尽最大努力，有时可能需要更长的时间。如果问题在一段时间后仍然存在，请联系Amazon Web Services 支持并提供亚马逊 CloudWatch支持的Amazon Config指标。有关这些指标的信息，请参阅Amazon Config使用情况和成功指标。

控制对的访问权限Amazon Config

Amazon Identity and Access Management是一项网络服务，可让 Amazon Web Services (Amazon) 客户管理用户和用户权限。

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对第三方身份提供商创建角色（联合身份验证）的说明进行操作。

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。

- （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

Amazon Config 术语和概念

为了帮助您了解，Amazon Config本主题介绍了一些主要概念。

目录

- Amazon Config 接口
  - Amazon Config 控制台
  - Amazon Config CLI
  - Amazon Config API
  - Amazon Config SDK
- 资源管理
  - Amazon 资源
  - 资源关系
- 配置记录器
- 传输通道
  - 配置项
  - 配置历史
  - 配置快照
  - 配置流
- Amazon Config 规则
  - 评估结果
  - 规则类型
  - 触发器类型
  - 评估模式

Amazon Config 接口

Amazon Config 控制台

您可以使用 Amazon Config 控制台管理服务。有关 Amazon Web Services 管理控制台 的更多信息，请参阅 Amazon Web Services 管理控制台

Amazon Config CLI

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

Amazon Config API

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

Amazon Config SDK

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

资源管理

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

Amazon 资源

Amazon 资源 是您使用、Amazon Web Services 管理控制台Amazon Command Line Interface（CLI）、Amazon 开发工具包或 Amazon 合作伙伴工具创建和管理的实体。Amazon 资源的示例包括 Amazon EC2 实例、安全组、Amazon VPC 和 Amazon Elastic Block Store。Amazon Config 使用其唯一标识符（例如，资源 ID 或 Amazon 资源名称（ARN））来参考每个资源。有关 Amazon Config 支持的资源类型列表，请参阅 支持的资源类型 Amazon Config

资源关系

Amazon Config 会查找您账户中的 Amazon 资源，然后创建 Amazon 资源关系图。例如，关系可能包括附加到与安全组 `sg-ef678hk` 关联的 Amazon EC2 实例 `i-a1b2c3d4` 的 Amazon EBS 卷。`vol-123ab45d`

有关更多信息，请参阅 支持的资源类型 Amazon Config

配置记录器

配置记录器以配置项的形式存储资源类型的配置更改。有关更多信息，请参阅 使用配置记录器

有两种类型的配置记录器。

类型	描述
客户管理的配置记录器	您管理的配置记录器。范围内的资源类型由您设置。默认情况下，客户管理的配置记录器会记录正在运行 Amazon Config 的 Amazon Web Services 区域内所有受支持的资源。
服务相关配置记录器	关联到特定 Amazon Web Services 服务的配置记录器。范围内的资源类型由相关服务设置。

传输通道

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

配置项

配置项 代表您账户中受支持的 Amazon 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，Amazon Config 就会创建配置项。例如，如果 Amazon Config 正在记录 Amazon S3 存储桶，则只要创建、更新或删除存储桶，Amazon Config 就会创建配置项。您也可以选择让 Amazon Config 以您设置的记录频率创建配置项。

有关更多信息，请参阅Components of a Configuration Item和记录频率。

配置历史

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

有关更多信息，请参阅查看合规性历史记录和查询合规性历史记录。

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 Amazon Config 控制台中选择一个时间点，并按照资源之间的关系浏览不同配置项的快照。

有关更多信息，请参阅传送配置快照、查看配置快照和示例配置快照。

配置流

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

Amazon Config 规则

Amazon Config 规则是一种合规性检查，可帮助您管理特定 Amazon 资源的理想配置设置。Amazon Config 用于评估资源配置是否遵从相关规则，并显示合规性结果。

评估结果

以下是 Amazon Config 规则四个可能的评估结果。

评估结果	描述
`COMPLIANT`	规则通过了合规性检查的条件。

评估结果	描述
NON_COMPLIANT	此规则未通过合规性检查的条件。
ERROR	其中一个必选/可选参数无效，或者类型不正确，或者格式不正确。
NOT_APPLICABLE	用于筛选出无法应用规则逻辑的资源。例如，alb-desync-mode-check 规则仅检查应用程序负载均衡器，而忽略网络负载均衡器和网关负载均衡器。

规则类型

有两种类型的规则。有关规则定义和规则元数据的结构的更多信息，请参阅 Amazon Config 规则的组成部分。

类型	描述	更多信息
托管规则	Amazon Config 创建的预定义、可自定义规则。	有关托管规则的列表，请参阅 Amazon Config 托管规则列表。
自定义规则	您从头开始创建的规则。有两种方法可以创建 Amazon Config 自定义规则：使用 Lambda 函数（Amazon Lambda 开发人员指南）和使用 Guard（Guard GitHub 存储库）。	有关更多信息，请参阅创建 Amazon Config 自定义策略规则和创建 Amazon Config 自定义 Lambda 规则。

触发器类型

将规则添加到账户后，Amazon Config 会将您的资源与规则的条件进行比较。完成这一初始评估后，Amazon Config 会在每次触发评估时继续执行评估。规则中会定义评估触发器，可以包括以下类型。

触发器类型	描述
配置更改	当存在与规则范围匹配的资源，并且资源配置发生变化时，Amazon Config 会对规则进行评估。在 Amazon Config 发送配置项更改通知后，评估便会运行。 通过定义规则的范围来选择哪些资源启动评估。范围可以包括： • 一个或多个资源类型 • 资源类型和资源 ID 的组合 • 标签键和值的组合 • 当创建、更新或删除任何记录的资源时 Amazon Config 在检测到与规则的范围匹配的资源发生更改时运行评估。您可以使用范围来定义哪些资源启动评估。
定期	Amazon Config 会按照您选择的频率运行规则评估（例如，每 24 小时）。
混合	有些规则既有配置更改也有定期触发器。对于这些规则，Amazon Config 会在检测到配置更改时以及按照您指定的频率评估您的资源。

评估模式

Amazon Config 规则有两种评估模式。

评估模式	描述
主动	使用主动评估在资源部署之前对其进行评估。这使您可以根据您所在区域的账户中的主动规则集，评估一组资源属性（如果用于定义 Amazon

评估模式	描述
	资源）是 COMPLIANT 还是 NON_COMPLIANT。 有关更多信息，请参阅评估模式。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 Amazon Config 托管规则列表。
侦查	使用侦查评估来评估已部署的资源。这允许您评估现有资源的配置设置。

> **Note**
>
> 主动规则不会修复标记为 NON_COMPLIANT 的资源，也不会阻止部署这些资源。

Amazon服务集成Amazon Config

Amazon Config支持与其他几项Amazon服务的集成。此列表并不详尽。

Amazon Organizations

您可以使用定义Amazon Organizations要用于的多账户、多区域数据聚合功能Amazon Config的账户。Amazon Organizations是一项账户管理服务，可帮助您将多个账户整合Amazon Web Services 账户到一个由您创建和集中管理的组织中。通过提供您的Amazon Organizations详细信息，您可以监控整个组织的合规状态。有关更多信息，请参阅 Amazon Organizations用户指南中的 Amazon Config和 Amazon Organizations。

Amazon Control Tower

Amazon Control TowerAmazon Config在所有注册的帐户上启用，以便它可以通过侦探控制来监控合规性、记录资源更改并将资源更改日志传送到日志存档帐户。有关更多信息，请参阅《Amazon Control Tower用户指南》中的使用Amazon Config监控资源更改。

Amazon CloudTrail

Amazon Config与集成Amazon CloudTrail，将配置更改与您账户中的特定事件相关联。您可以使用 CloudTrail 日志来获取引发变更的事件的详细信息，包括谁发出了请求、何时以及来自哪个 IP 地址。

您可以从 CloudTrail 控制台导航到Amazon Config时间轴，查看与您的Amazon API 活动相关的配置更改。

有关更多信息，请参阅Amazon Config开发人员指南Amazon CloudTrail中的使用记录Amazon Config API 调用和Amazon CloudTrail用户指南中的使用控制台为Amazon Config配置项目创建事件数据存储。

Amazon Security Hub CSPM

Amazon Security Hub CSPM集中来自其他Amazon服务的安全检查，包括Amazon Config规则。Security Hub 会启用并控制Amazon Config规则，以验证您的资源配置是否符合最佳实践。Amazon Config在 Security Hub CSPM 要对环境资源进行安全检查的所有区域的所有账户上启用该选项。有关更多信息，请参阅《Amazon Security Hub CSPM用户指南》中的将调查发现发送到 Security Hub 的Amazon服务。

> **某些与 Security Hub CSPM 相关的规则是周期性的，不依赖于配置项目**
>
> 一些与 Security Hub CSPM 相关的规则是定期的。这些规则不依赖于配置项（CI），因此可在配置记录器未启用的情况下运行。
> 这意味着，如果您查看规则页面，其中不会列出 CI 或支持的资源。如果您选择资源 ID，将会看到以下错误：`The provided resource ID and resource type cannot be found`。这是预料之中的行为。

Amazon Trusted Advisor

Amazon Config托管规则支持对所有类别Trusted Advisor进行一组检查。启用某些托管规则后，相应的Trusted Advisor检查将自动启用。要查看哪些Trusted Advisor检查由特定的Amazon Config托管规则提供支持，请参阅Amazon Web Services 支持用户指南中的Amazon Trusted Advisor检查参考。

有Amazon商业支持、Amazon企业入口和Amazon企业支持计划的客户可以使用Amazon Config强力支票。如果您启用Amazon Config了其中Amazon一个 Support 计划，则会自动看到由相应部署的Amazon Config托管规则支持的推荐。

> **不允许刷新请求，也无法排除资源**
>
> 这些检查的结果会根据变更触发的托管规则更新自动刷新。Amazon Config不允许刷新请求。您目前无法从这些检查中排除资源。

有关更多信息，请参阅《Amazon Web Services 支持用户指南》Amazon Config中的 “查看由其支持的Trusted Advisor支票”。

Amazon Audit Manager

您可以使用 Audit Manager 捕获Amazon Config评估作为审计证据。创建或编辑自定义控件时，可以将一个或多个Amazon Config规则指定为证据收集的数据源映射。Amazon Config根据这些规则执行合规性检查，然后 Audit Manager 将结果报告为合规性检查证据。有关更多信息，请参阅《Amazon Audit Manager用户指南》中的 Amazon Audit Manager支持的Amazon Config规则。

Amazon Systems Manager

Amazon Config与 Systems Manager 集成，可在本地环境中记录亚马逊 EC2 实例和服务器上软件的配置更改。通过这种集成，您可以了解操作系统 (OS) 配置、系统级更新、已安装的应用程序、网络配置等。Amazon Config还提供了操作系统和系统级配置更改的历史记录以及为 Amazon EC2 实例记录的基础设施配置更改。您可以从 Systems Manager 控制台导航到Amazon Config时间轴，查看托管亚马逊 EC2 实例的配置更改。您可以使用Amazon Config查看 Systems Manager 库存历史记录并跟踪所有托管实例的更改。

有关更多信息，请参阅《Amazon Systems Manager用户指南》中的 “与Amazon服务集成 | 管理和治理”、“Amazon Config配置记录器” 和 “Amazon Config一致性包部署”。

Amazon Firewall Manager

要使用 Firewall Manager，必须Amazon Config为每个Amazon Organizations成员帐户启用防火墙管理器。创建新应用程序时，Firewall Manager 是构建防火墙规则、创建安全策略并一致实施这些规则的唯一服务。有关更多信息，请参阅Amazon WAFAmazon Firewall Manager、和Amazon Shield Advanced开发者指南Amazon Config中的启用。

> **Note**
>
> Firewall Manager 依赖连续记录来监控您的资源。如果您使用的是 Firewall Manager，建议您将记录频率设置为“持续”。有关连续录制和每日录制的更多信息，请参阅录制频率。

Amazon EC2 专用主机

Amazon Config与 Amazon EC2 专用主机集成以评估许可合规性。Amazon Config记录实例何时在专用主机上启动、停止或关闭，并将此信息与与软件许可相关的主机和实例级别信息（例如主机

ID、Amazon 机器映像 (AMI) IDs、套接字数量和物理内核）配对。这可以帮助您Amazon Config用作许可证报告的数据源。您可以从 Amazon EC2 专用主机控制台导航到Amazon Config时间轴，查看您的亚马逊 EC2 专用主机的配置更改。

有关更多信息，请参阅《适用于 Linux 实例的 Amazon Elastic Compute Cloud 用户指南》中的跟踪配置更改或《适用于 Windows 实例的 Amazon Elastic Compute Cloud 用户指南》中的跟踪配置更改。

应用程序负载均衡器

Amazon Config与 Elastic Load Balancing (ELB) 服务集成，可记录应用程序负载均衡器的配置更改。Amazon Config还包括与相关 Amazon EC2 安全组和子网的关系。 VPCs您可以使用这些信息进行安全分析和故障排除。例如，您可以随时查看哪些安全组与您的应用程序负载均衡器相关联。您可以从 ELB 控制台导航到Amazon Config时间轴，查看应用程序负载均衡器的配置更改。

Amazon CodeBuild

Amazon Config提供了您的Amazon资源清单以及这些资源的配置更改历史记录。Amazon Config支持 Amazon CodeBuild；作为一种Amazon资源，这意味着该服务可以跟踪您的 CodeBuild 项目。有关更多信息，请参阅《Amazon CodeBuild用户指南》中的 “Amazon Config与 CodeBuild 示例一起使用”。

Amazon X-Ray

Amazon X-Ray与集成Amazon Config以记录对 X-Ray 加密资源所做的配置更改。您可以使用Amazon Config清点 X-Ray 加密资源、审计 X-Ray 配置历史记录以及根据资源更改发送通知。有关更多信息，请参阅《Amazon X-Ray开发人员指南》中的使用Amazon Config跟踪 X-Ray 加密配置更改。

Amazon 服务管理连接器

f Amazon 服务管理连接器 or ServiceNow 可以使用聚合器同步来自多个账户和地区的Amazon Config数据。有关更多信息，请参阅《Amazon 服务管理连接器管理员指南》Amazon Config ServiceNow中的 “集成”。

Amazon API Gateway

您可以使用Amazon Config记录对 API Gateway API 资源所做的配置更改，并根据资源更改发送通知。维护 API Gateway 资源的配置更改历史记录对于运行问题排查、审计与合规性使用案例非常有用。有关更多信息，请参阅《API Gateway 开发人员指南》中的使用Amazon Config监控 API Gateway API 配置。

Region Support Amazon Config

注意事项

的某些功能 Amazon Config 仅在支持的部分 Amazon 区域中 Amazon Config 受支持。

资源管理

- 有关哪些区域支持哪些 Amazon 资源类型的列表，请参阅按区域可用性划分的资源覆盖率。

Amazon Config Rules

- 有关哪些区域支持哪些 Amazon Config 规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。
- 有关支持组织部署规则的区域列表，请参阅组织 Amazon Config 规则 | Region Suppor t。

聚合器

高级查询

- 有关支持高级查询的区域列表，请参阅高级查询 | 区域支持。
- 有关支持适用于高级查询的自然语言查询处理器的区域列表，请参阅适用于高级查询的自然语言查询处理器 | 区域支持。

受支持区域列表

下表列出了您可以启用的 Amazon 区域 Amazon Config。

区域名称	区域	端点	协议	
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS	
美国东部（弗吉尼	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS	

区域名称	区域	端点	协议
亚州北部）			
美国西部（北加利福尼亚）	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
亚太地区（马来西亚）	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（新西兰）	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（台北）	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
亚太地区（泰国）	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
亚太地区（东京）	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
中国（北京）	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS

区域名称	区域	端点	协议	
中国（宁夏）	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS	
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
墨西哥（中部）	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议	
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS	
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

Amazon Config 的服务限制

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

有关 Amazon 中的其他限制的信息，请参阅 Amazon 服务限制。

资源标签

描述	限制值	能否增加
每个资源的最大标签数	50	否

Amazon Config 规则

描述	限制值	能否增加
最大 Amazon Config 规则数（每个区域、每个账户）	1000	否

单个账户合规包

描述	限制值	能否增加
每个账户的最大合规包数	50	不可以

描述	限制值	能否增加
每个合规包最多 Amazon Config 条规则	130	否

> **Note**
>
> 合规包中的 Amazon Config 规则计入每账户每区域的最大数量 Amazon Config 规则限制。

组织合规包

描述	限制值	能否增加
每个组织的最大合规包数	50	不可以
每个组织合规包的最大 Amazon Config 规则数	130	否

> **Note**
>
> 在组织级别部署计入子账户限制。合规包中的 Amazon Config 规则计入每账户每区域的最大数量 Amazon Config 规则限制。

聚合器

描述	限制值	能否增加
最大配置聚合器数	50	可以
聚合器中的最大账户数	10000	否
所有聚合器每周添加或删除的最大账户数量	1000	是

> **Note**
>
> 组织级聚合器和个人账户聚合器都计入配置聚合器的最大数量限制。

高级查询

描述	限制值	能否增加
单个账户和一个区域中保存的查询的最大数量	300	是

Amazon Config 的补充信息和相关资源

下列相关资源在您使用此服务的过程中会有所帮助。

- Amazon Config – 提供 Amazon Config 相关信息的主要网页。
- Amazon Config 定价
- 技术方面常见问题
- Amazon Config 规则开发工具包（RDK）– 一种开源工具，可帮助您设置，Amazon Config编写规则，然后使用各种 Amazon 资源类型对其进行测试。
- 合作伙伴 – 链接到合作伙伴的产品，这些产品与 Amazon 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。

- 入门资源中心 – 了解如何设置、Amazon Web Services 账户加入 Amazon 社区和启动您的第一个应用程序。
- Amazon Web Services 支持 中心 – 用于创建和管理 Amazon Web Services 支持 案例的中心。还提供指向其他有用资源的链接，如论坛、技术常见问题、服务运行状况以及Amazon Trusted Advisor。
- Amazon Web Services 支持 – 提供有关 Amazon Web Services 支持 的信息的主要网页，这是一个一对一的快速响应支持渠道，可以帮助您在云中构建和运行应用程序。
- 联系我们 – 用于查询有关 Amazon 账单、账户、事件、滥用和其他问题的中央联系点。
- Amazon 网站条款 – 有关我们的版权和商标、您的账户、许可、网站访问和其他主题的详细信息。

Amazon适用于 的 软件开发工具包Amazon Config

Amazon 软件开发工具包使用户可以更轻松地构建应用程序，以对经济高效、可扩展而又可靠的 Amazon 基础设施服务进行访问。Amazon 软件开发工具包是可下载的单个软件包，其中包含库、代码示例和参考文档，您可以在几分钟内开始使用。下表列出了可用的软件开发工具包和第三方库，以便您以编程方式访问。Amazon Config

访问类型	描述
Amazon SDK	Amazon 提供以下软件开发工具包： • 适用于 C++ 文档的 Amazon 开发工具包 • Amazon Mobile SDK for iOS 文档 • 适用于 Go 文档的 Amazon 开发工具包 • 适用于 Java 的 Amazon SDK 文档 • 适用于 JavaScript 文档的 Amazon 开发工具包 • 适用于 .NET 的 Amazon SDK 文档 • 适用于 PHP 的 Amazon SDK 文档 • Amazon SDK for Python (Boto) 文档 • 适用于 Ruby 的 Amazon SDK 文档
第三方库	Amazon 开发人员社区中的开发人员还会提供他们自己的库，您可以在以下 Amazon 开发人员中心获取这些资源： • Amazon Java 开发人员中心 • Amazon JavaScript 开发人员中心 • AmazonPHP 开发人员中心 • Amazon Python 开发者中心 • Amazon Ruby 开发人员中心 • Amazon Windows 和 .NET 开发人员中心

入门Amazon Config

Amazon Config提供了中Amazon资源配置的详细视图Amazon Web Services 账户。借Amazon Config助，您可以查看配置和Amazon资源之间关系的变化，浏览资源配置历史记录，并使用规则来确定合规性。有关更多信息，请参阅什么是Amazon Config？ 以及Amazon Config工作原理。

报名参加Amazon

主题

- 注册获取Amazon Web Services 账户
- 保护 IAM 用户

注册获取Amazon Web Services 账户

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

报名参加Amazon Web Services 账户

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

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

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

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

保护 IAM 用户

注册后Amazon Web Services 账户，开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的Amazon Web Services 账户资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在你的 IAM 用户中创建Amazon Web Services 账户
- 适用于Amazon资源的访问权限管理
- 基于 IAM 身份的策略示例

入门方法Amazon Config

注册后Amazon Web Services 账户，您可以开始Amazon Config使用Amazon Web Services 管理控制台、Amazon CLI 或Amazon SDKs。

- 使用控制Amazon Config台进行设置
- Amazon Config使用进行设置Amazon CLI
- 在Amazon SDK 中使用Amazon Config服务

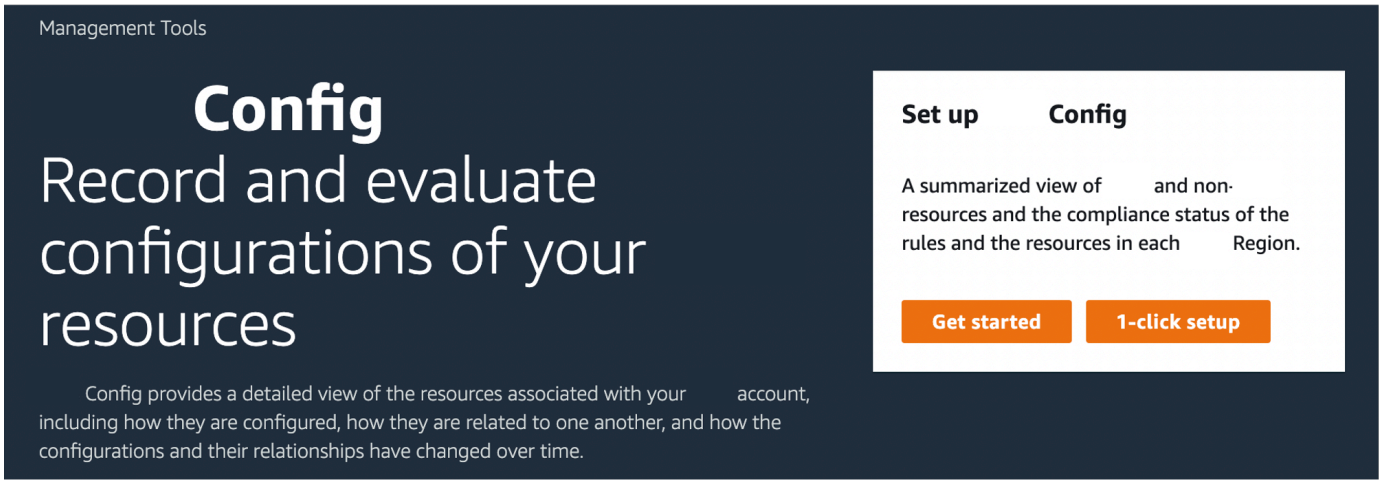
使用控制台设置 Amazon Config

Amazon Web Services 管理控制台提供了一个快速、简化的 Amazon Config 设置流程。

设置

使用控制台设置 Amazon Config

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



3. 根据 Amazon 最佳实践选择 一键设置以启动。Amazon Config您也可以选择开始使用来完成更详细的设置过程。

主题

- 一键设置 Amazon Config
- 的手动设置Amazon Config

一键设置 Amazon Config

通过减少手动选择的数量，Amazon Config 一键设置有助于简化 Amazon Config 控制台客户的入门流程。要完成设置过程的所有手动选择，请参阅手动设置。

使用一键设置在控制台上设置 Amazon Config

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 选择一键设置。

设置页面包括三个步骤，但是通过一键设置工作流，您将被自动定向到步骤 3（查看）。下面详细列出了这些步骤。

- 设置：选择 Amazon Config 控制台记录资源和角色的方式，并选择配置历史记录和配置快照文件的发送位置。

- 规则：对于支持 Amazon Config 规则的，Amazon Web Services 区域本步骤可供您配置可以添加到账户的初始托管规则。设置后，Amazon Config 会根据您选择的规则来评估您的 Amazon 资源。设置完成后，可以创建其他规则，您账户中的现有规则也会更新。
- 查看：验证您的设置详细信息。

步骤 1：设置

记录策略

为您选择了记录所有具有可自定义覆盖的资源类型的选项。Amazon Config 将记录该区域支持的所有当前和未来资源类型。有关更多信息，请参阅支持的资源类型。

- 默认设置

  默认记录频率已设置为持续。这意味着每当发生更改时，Amazon Config 都会持续记录配置更改。

  Amazon Config 还支持将记录频率设置为每日的选项。如果您在设置之后选择该选项，将会收到代表过去 24 小时内资源最新状态的配置项（CI），前提是它与之前记录的 CI 不同。有关更多信息，请参阅记录频率。

  > **Note**
  >
  > Amazon Firewall Manager 依赖连续记录来监控您的资源。如果您使用的是 Firewall Manager，建议您将记录频率设置为“持续”。

- 覆盖设置 – 可选

  您可以选择在设置完成后覆盖特定资源类型的记录频率，或从记录中排除特定资源类型。要覆盖默认设置，请在 Amazon Config 控制台的左侧导航栏中选择设置，然后选择编辑。

记录资源时的注意事项

大量 Amazon Config 评估

您可能会注意到，在最初使用 Amazon Config 记录的一个月中，账户活动会多于随后的几个月。在初始引导过程中，Amazon Config 会对您账户中选择的、需要 Amazon Config 记录的所有资源进行评估。

如果您运行的是临时工作负载，则可能会看到 Amazon Config 中的活动增加，因为它会记录与创建和删除这些临时资源相关的配置更改。临时工作负载 是临时使用在需要时加载和运行的计算资源。示例

包括 Amazon Elastic Compute Cloud（Amazon EC2）竞价型实例、Amazon EMR 任务和。Amazon Auto Scaling如果您想避免因运行临时工作负载而导致活动增加，则可以设置配置记录器，将这些资源类型排除在记录范围之外，或者在单独的账户中运行这些类型的工作负载，同时将 Amazon Config 关闭，以避免增加配置记录和规则评估。

全局资源类型 | Aurora 全局集群最初包含在记录范围内

`AWS::RDS::GlobalCluster` 资源类型将记录在已启用配置记录器的所有受支持 Amazon Config 区域中。

如果您不想在所有已启用的区域中记录，`AWS::RDS::GlobalCluster`可以在设置完成后将此资源类型排除在记录范围之外。在左侧导航栏中选择设置，然后选择编辑。从编辑菜单转到记录方法部分的覆盖设置，选择 `AWS::RDS::GlobalCluster`，然后选择“从记录中排除”覆盖方法。

全局资源类型 | IAM 资源类型最初不包含在记录范围内

为了帮您降低成本，“所有全局记录的 IAM 资源类型”最初都不包含在记录范围内。此捆绑包包括 IAM 用户、组、角色和客户管理型策略。选择移除以删除覆盖，并将这些资源包含在您的记录范围内。

此外，Amazon Config 在 2022 年 2 月之后提供支持的区域中，无法记录以下全局 IAM 资源类型：`AWS::IAM::User`、`AWS::IAM::Group`、`AWS::IAM::Role` 和 `AWS::IAM::Policy` 有关这些区域的列表，请参阅记录 Amazon 资源 | 全球资源。

数据治理

在这部分中，系统为您选择的默认数据留存期是将 Amazon Config 数据保留 7 年（2557 天）。

已为您选择了使用现有 Amazon Config 服务相关角色选项并将其设置为 Amazon Config 角色。服务相关角色由 Amazon Config 预定义，并包含该服务调用其他 Amazon 服务所需的一切权限。

传送方式

在本部分中为您选择了从您的账户中选择一个存储桶选项。此选项将默认为您账户中以 `config-bucket-`*`accountid`* 格式命名的存储桶。例如。`config-bucket-012345678901`如果您没有以这种格式创建存储桶，则会为您创建一个这种格式的存储桶。如果希望创建自己的存储桶，请参阅《Amazon Simple Storage Service 用户指南》中的创建存储桶。

有关 S3 存储桶的更多信息，请参阅《Amazon Simple Storage Service（Amazon S3）用户指南》中的存储桶概述。

步骤 2：规则

根据 Amazon 托管规则，此步骤未为您选择任何规则。但我们鼓励您在完成账户设置后创建和更新规则。

第 3 步：查看

查看您的 Amazon Config 设置详细信息。您可以返回编辑每个部分中所做的更改。要完成设置，Amazon Config请选择确认。

的手动设置Amazon Config

使用 Get started 工作流程，您可以完成设置过程的所有手动选择以开始使用Amazon Config控制台。有关简化的入门流程，请参阅一键设置。

使用 “入门” 在控制台上Amazon Config进行设置

1. 登录Amazon Web Services 管理控制台并在家中打开https://console.aws.amazon.com/config/主Amazon Config机。
2. 选择开始。

设置页面包括三个步骤。下文详细介绍了您选择入门之后的该过程。

- 设置：选择Amazon Config控制台记录资源和角色的方式，并选择配置历史记录和配置快照文件的发送位置。
- 规则：对于Amazon Web Services 区域该支持Amazon Config规则，您可以通过此步骤配置可以添加到您的账户的初始托管规则。设置完成后，Amazon Config将根据您选择的规则评估您的Amazon资源。设置完成后，可以创建其他规则，您账户中的现有规则也会更新。
- 查看：验证您的设置详细信息。

步骤 1：设置

记录策略

在记录方法部分，选择记录策略。您可以指定Amazon Config要记录的Amazon资源。

All resource types with customizable overrides

设置Amazon Config为记录该区域所有当前和 future 支持的资源类型的配置更改。您可以覆盖特定资源类型的记录频率，也可以从记录中排除特定资源类型。有关更多信息，请参阅支持的资源类型。

- 默认设置

  为所有当前和未来支持的资源类型配置默认记录频率。有关更多信息，请参阅记录频率。

  - 连续录制 —Amazon Config每当发生更改时，都会持续记录配置更改。
  - 每日记录 - 您会收到代表过去 24 小时内资源的最新状态的配置项（CI），前提是它与之前记录的 CI 不同。

  > **Note**
  >
  > Amazon Firewall Manager依赖于持续录制来监控您的资源。如果您使用的是 Firewall Manager，建议您将记录频率设置为“持续”。

- 覆盖设置

  覆盖特定资源类型的记录频率，或从记录中排除特定资源类型。如果您更改某一资源类型的记录频率或停止记录某一资源类型，则已记录的配置项会保持不变。

Specific resource types

设置Amazon Config为仅记录您指定的资源类型的配置更改。

- 特定的资源类型

  选择要记录的资源类型及其频率。有关更多信息，请参阅记录频率。

  - 连续录制 —Amazon Config每当发生更改时，都会持续记录配置更改。
  - 每日记录 - 您会收到代表过去 24 小时内资源的最新状态的配置项（CI），前提是它与之前记录的 CI 不同。

  > **Note**
  >
  > Amazon Firewall Manager依赖于持续录制来监控您的资源。如果您使用的是 Firewall Manager，建议您将记录频率设置为“持续”。

如果您更改某一资源类型的记录频率或停止记录某一资源类型，则已记录的配置项会保持不变。

记录资源时的注意事项

Amazon Config评估次数多

与随后的几个月相比，您可能会注意到，在使用Amazon Config 记录的第一个月份中，您的账户活动有所增加。在初始引导过程中，Amazon Config会对您账户中您选择Amazon Config要记录的所有资源进行评估。

如果您运行的是临时工作负载，则可能会看到Amazon Config中的活动增加，因为它会记录与创建和删除这些临时资源相关的配置更改。临时工作负载 是临时使用在需要时加载和运行的计算资源。示例包括亚马逊弹性计算云 (Amazon EC2) 竞价型实例、亚马逊 EMR 任务和Amazon Auto Scaling。如果您想避免因运行临时工作负载而导致活动增加，则可以设置配置记录器，将这些资源类型排除在记录范围之外，或者在单独的账户中运行这些类型的工作负载，同时将Amazon Config关闭，以避免增加配置记录和规则评估。

Considerations: All resource types with customizable overrides

全局记录的资源类型 | Aurora 全局集群最初包含在记录范围内

`AWS::RDS::GlobalCluster`资源类型将在启用配置记录器的所有支持Amazon Config区域中进行记录。

如果您不想在所有已启用的区域中记录，`AWS::RDS::GlobalCluster`请选择“Amazon RDS GlobalCluster”，然后选择“从记录中排除”覆盖方法。

全局资源类型 | IAM 资源类型最初不包含在记录范围内

为了帮您降低成本，全局 IAM 资源类型最初将不包含在记录范围内。此捆绑包包括 IAM 用户、组、角色和客户管理型策略。选择移除以删除覆盖，并将这些资源包含在您的记录范围内。

此外，全球 IAM 资源类型（`AWS::IAM::User`、`AWS::IAM::Group`、`AWS::IAM::Role`、和`AWS::IAM::Policy`）不能记录在 2022 年 2 月Amazon Config之后支持的区域中。有关这些区域的列表，请参阅录制Amazon资源 | 全球资源。

限制

您可以添加最多 100 项频率覆盖和 600 项排除覆盖。

无法为以下资源类型指定每日记录：

- AWS::Config::ResourceCompliance
- AWS::Config::ConformancePackCompliance
- AWS::Config::ConfigurationRecorder

Considerations: Specific resource types

区域可用性

在指定Amazon Config要跟踪的资源类型之前，请检查按区域可用性划分的资源覆盖率，以查看您设置的Amazon区域是否支持该资源类型Amazon Config。如果至少有一个区域支持某种资源类型，则即使您设置的区域不支持指定的资源类型Amazon Config，您也可以在支持的所有Amazon区域中启用该资源类型的记录Amazon Config。Amazon Config

限制

如果所有资源类型的频率都相同，则没有限制。如果至少将一种资源类型设置为“持续”，则最多可以添加 100 种频率为“每日”的资源类型。

以下资源类型不支持“每日”频率：

- AWS::Config::ResourceCompliance
- AWS::Config::ConformancePackCompliance
- AWS::Config::ConfigurationRecorder

数据治理

- 对于数据保留期，选择默认保留期以将Amazon Config数据保留 7 年 (2557)，或者为记录的项目设置自定义保留期。Amazon Config

  Amazon Config允许您通过为自己的数据指定保留期来删除数据ConfigurationItems。指定保留期后，Amazon Config会将您的 ConfigurationItems 保留指定的时间段。您可以选择最少 30 天到最长 7 年（2557 天）之间的时间段。Amazon Config删除早于您指定保留期的数据。
- 对于的 IAM 角色Amazon Config，请从您的账户中选择现有的Amazon Config服务相关角色或一个 IAM 角色。
  - 服务相关角色由服务预定义Amazon Config，包括该服务调用其他Amazon服务所需的所有权限。

> **Note**
>
> 推荐：使用服务相关角色
> 建议您使用服务相关角色。服务相关角色可添加Amazon Config按预期运行所需的所有必要权限。

- 否则，请从现有的角色和权限策略中选择一个 IAM 角色。

> **Note**
>
> 策略与合规结果
> 在中管理@@ 的 IAM 策略和其他策略Amazon Organizations可能会影响是否Amazon Config有权记录资源的配置更改。此外，规则会直接评估资源的配置，且执行评估时不会考虑这些策略。确保现行策略与您打算使用Amazon Config的方式保持一致。
> 重用 IAM 角色时保留最低权限
> 如果您使用的是使用Amazon Security Hub CSPM或之类的Amazon服务Amazon ConfigAmazon Control Tower，并且已经创建了 IAM 角色，请确保您在设置时使用的 IAM 角色Amazon Config保持与先前存在的 IAM 角色相同的最低权限。您必须这样做才能确保其他Amazon服务继续按预期运行。
> 例如，如果Amazon Control Tower拥有允许Amazon Config读取 S3 对象的 IAM 角色，请确保向设置时使用的 IAM 角色授予相同的权限Amazon Config。否则，它可能会干扰Amazon Control Tower工作方式。

传送方式

- 对于传送方式，选择Amazon Config将配置历史记录和配置快照文件发送到的 S3 存储桶：
  - 创建存储桶 – 对于 S3 存储桶名称，键入 S3 存储桶的名称。

    您键入的名称在 Amazon S3 中所有现有的存储桶名称中必须唯一。添加前缀（例如，您所在组织的名称）是确保唯一性的一种方法。存储桶创建完毕后，您无法更改其名称。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的存储桶限制。
  - 从您的账户选择一个存储桶 – 对于 S3 存储桶名称，选择您的首选存储桶。
  - 从另一账户选择存储桶 – 对于 S3 存储桶名称，键入存储桶名称。

> **Note**
>
> 存储桶权限
> 如果您从其他账户中选择存储桶，则该存储桶必须具有授予访问权限的策略Amazon Config。有关更多信息，请参阅 Amazon Config 传送渠道的 Amazon S3 存储桶的权限。

- 对于 Amazon SNS 主题，选择将配置更改和通知流式传输到 Amazon SNS 主题，以便Amazon Config发送配置历史传送、配置快照传输和合规性等通知。
- 如果您选择Amazon Config直播某个 Amazon SNS 主题，请选择目标主题：
  - 创建主题 – 对于主题名称，键入您的 SNS 主题的名称。
  - 从您的账户选择一个主题 – 对于主题名称，选择您的首选主题。
  - 从另一个账户选择一个主题 – 对于主题 ARN，键入主题的 Amazon 资源名称（ARN）。如果您从其他账户中选择一个主题，则该主题必须具有授予访问权限的策略Amazon Config。有关更多信息，请参阅 Amazon SNS 主题的权限。

> **Note**
>
> Amazon SNS 主题的区域
> Amazon SNS 主题必须与您设置的区域位于同一区域。Amazon Config

步骤 2：规则

如果您在支持规则Amazon Config的地区进行设置，请选择下一步。

第 3 步：查看

查看您的Amazon Config设置详情。您可以返回编辑每个部分中所做的更改。选择 “确认” 以完成设置Amazon Config。

有关更多信息

有关在账户中查找现有资源和了解资源配置的信息，请参阅查找资源、查看合规信息和查看合规历史记录。

您也可以使用 Amazon 简单队列服务以编程方式监控Amazon资源。有关更多信息，请参阅 使用 Amazon SQS 监控Amazon资源变化。

使用 Amazon Config 设置 Amazon CLI

Amazon CLI 是用于管理 Amazon 服务的统一工具。如果您仅使用一种工具进行下载和配置，则可通过命令行控制多个 Amazon 服务并使用脚本来自动执行这些服务。有关 Amazon CLI 的更多信息以及 Amazon CLI 工具的安装说明，请参阅《Amazon Command Line Interface 用户指南》中的以下内容。

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

如有必要，请输入 `aws configure` 以将 Amazon CLI 配置为使用提供 Amazon Config 的 Amazon 区域。

设置

请参阅以下主题以使用 Amazon Config 设置。Amazon CLI

主题

- 使用进行设置 Amazon Config 的先决条件 Amazon CLI
- 通过 Amazon CLI 使用客户管理的配置记录器启动 Amazon Config
- 验证是否已使用 Amazon CLI 成功启动 Amazon Config

使用进行设置 Amazon Config 的先决条件 Amazon CLI

在设置 Amazon 之前 Amazon CLI，您需要创建一个 Amazon S3 存储桶、一个 Amazon SNS 主题和一个将附加策略作为先决条件的 IAM 角色。然后，您可以使用 Amazon CLI 为指定存储桶、主题和角色 Amazon Config。请按照以下步骤设置 Amazon Config的先决条件。

主题

- 步骤 1：创建 Amazon S3 存储桶
- 第 2 步：创建 Amazon SNS 主题
- 步骤 3：创建 IAM 角色

步骤 1：创建 Amazon S3 存储桶

如果您的账户中已存在 Amazon S3 存储桶，并且您想使用该存储桶，请跳过此步骤并转至。第 2 步：创建 Amazon SNS 主题

使用 S3 控制台

创建存储桶

1. 打开 Amazon S3 控制台，网址为 https://console.aws.amazon.com/s3/。
2. 选择创建桶。
3. 在 Bucket name（桶名称）中，输入符合 DNS 标准的桶名称。

   桶名称必须满足以下要求：

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

   创建存储桶后，便无法再更改其名称。请确保您选择的存储桶名称在 Amazon S3 中所有现有存储桶名称中唯一。有关存储桶命名规则和约定的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的存储桶约束和限制。

   > **Important**
   >
   > 避免在存储桶名称中包含敏感信息。存储桶名称在指向存储桶 URLs 中对象的位置中可见。

4. 在区域中，选择您想要存储桶所在的 Amazon 区域。

   请选择一个靠近您的区域可最大程度地减少延迟和成本以及满足法规要求。在某一区域存储的对象将一直留在该区域，除非您特意将其转移到其他区域。有关 Amazon S3 Amazon 区域的列表，请参阅中的Amazon 服务终端节点Amazon Web Services 一般参考。

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

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

6. （可选）如果要启用 S3 对象锁定：

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

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

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

有关 S3 对象锁定功能的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的使用 Amazon S3 对象锁定以锁定对象。

7. 选择 创建存储桶 。

使用 Amazon SDKs

使用创建存储桶时，必须创建一个客户端，然后使用该客户端发送创建存储桶的请求。 Amazon SDKs 作为最佳做法，您应在同一 Amazon Web Services 区域中创建客户端和桶。如果您在创建客户端或桶时未指定区域，Amazon S3 将使用默认区域美国东部（弗吉尼亚北部）。

要创建用于访问双栈端点的客户端，必须指定。 Amazon Web Services 区域有关更多信息，请参阅 Amazon S3 双堆栈端点。有关可用区域的列表 Amazon Web Services 区域，请参阅中的区域和终端节点Amazon Web Services 一般参考。

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

这些 Amazon SDK 代码示例执行以下任务：

- 通过明确指定 Amazon Web Services 区域创建客户端 – 在本示例中，客户端使用 `s3.us-west-2.amazonaws.com` 终端节点与 Amazon S3 通信。您可以指定任意。 Amazon Web Services 区域有关列表 Amazon Web Services 区域，请参阅《Amazon 一般参考》中的区域和终端节点。

- 通过仅指定桶名称来发送创建桶请求 — 客户端向 Amazon S3 发送请求，请求在您创建客户端的区域中创建桶。
- 检索有关桶位置的信息 — Amazon S3 将桶位置信息存储在与桶关联的位置子资源中。

以下代码示例演示如何使用 `CreateBucket`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
        /// <param name="client">An initialized Amazon S3 client object.</param>
        /// <param name="bucketName">The name of the bucket to create.</param>
        /// <returns>A boolean value representing the success or failure of
        /// the bucket creation process.</returns>
        public static async Task<bool> CreateBucketAsync(IAmazonS3 client, string
bucketName)
        {
            try
            {
                var request = new PutBucketRequest
                {
                    BucketName = bucketName,
                    UseClientRegion = true,
                };

                var response = await client.PutBucketAsync(request);
                return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
            }
            catch (AmazonS3Exception ex)
            {
                Console.WriteLine($"Error creating bucket: '{ex.Message}'");
```

```
                return false;
            }
        }
```

创建一个启用对象锁定的存储桶。

```
    /// <summary>
    /// Create a new Amazon S3 bucket with object lock actions.
    /// </summary>
    /// <param name="bucketName">The name of the bucket to create.</param>
    /// <param name="enableObjectLock">True to enable object lock on the
bucket.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> CreateBucketWithObjectLock(string bucketName, bool
enableObjectLock)
    {
        Console.WriteLine($"\tCreating bucket {bucketName} with object lock
{enableObjectLock}.");
        try
        {
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

            return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine($"Error creating bucket: '{ex.Message}'");
            return false;
        }
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考CreateBucket中的。

Bash

Amazon CLI 使用 Bash 脚本

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
##############################################################################
# function iecho
#
# This function enables the script to display the specified text only if
# the global variable $VERBOSE is set to true.
##############################################################################
function iecho() {
  if [[ $VERBOSE == true ]]; then
    echo "$@"
  fi
}

##############################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
##############################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

##############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
```

```
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function create_bucket"
    echo "Creates an Amazon S3 bucket. You must supply a bucket name:"
    echo "  -b bucket_name    The name of the bucket. It must be globally
 unique."
    echo "  [-r region_code]    The code for an AWS Region in which the bucket is
 created."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

  if [[ -z "$bucket_name" ]]; then
    errecho "ERROR: You must provide a bucket name with the -b parameter."
    usage
    return 1
  fi
```

```
  local bucket_config_arg
  # A location constraint for "us-east-1" returns an error.
  if [[ -n "$region_code" ]] && [[ "$region_code" != "us-east-1" ]]; then
    bucket_config_arg="--create-bucket-configuration LocationConstraint=
$region_code"
  fi

  iecho "Parameters:\n"
  iecho "    Bucket name:   $bucket_name"
  iecho "    Region code:   $region_code"
  iecho ""

  # If the bucket already exists, we don't want to try to create it.
  if (bucket_exists "$bucket_name"); then
    errecho "ERROR: A bucket with that name already exists. Try again."
    return 1
  fi

  # shellcheck disable=SC2086
  response=$(aws s3api create-bucket \
    --bucket "$bucket_name" \
    $bucket_config_arg)

  # shellcheck disable=SC2181
  if [[ ${?} -ne 0 ]]; then
    errecho "ERROR: AWS reports create-bucket operation failed.\n$response"
    return 1
  fi
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考CreateBucket中的。

C++

SDK for C++

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
bool AwsDoc::S3::createBucket(const Aws::String &bucketName,
                              const Aws::S3::S3ClientConfiguration &clientConfig)
 {
    Aws::S3::S3Client client(clientConfig);
    Aws::S3::Model::CreateBucketRequest request;
    request.SetBucket(bucketName);

    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

 Aws::S3::Model::BucketLocationConstraintMapper::GetBucketLocationConstraintForName(
                        clientConfig.region));
        request.SetCreateBucketConfiguration(createBucketConfig);
    }

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: createBucket: " <<
                  err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    } else {
        std::cout << "Created bucket " << bucketName <<
                  " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- 有关 API 的详细信息，请参阅 适用于 C++ 的 Amazon SDK API 参考CreateBucket中的。

CLI

Amazon CLI

示例 1：创建存储桶

以下 `create-bucket` 示例创建一个名为 `amzn-s3-demo-bucket` 的存储桶：

```
aws s3api create-bucket \
```

```
    --bucket amzn-s3-demo-bucket \
    --region us-east-1
```

输出：

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

有关更多信息，请参阅《Amazon S3 用户指南》中的创建存储桶。

示例 2：创建带有强制拥有者的存储桶

以下 create-bucket 示例创建一个名为 amzn-s3-demo-bucket 的存储桶，该存储桶对于 S3 对象所有权使用强制存储桶拥有者设置。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region us-east-1 \
    --object-ownership BucketOwnerEnforced
```

输出：

```
{
    "Location": "/amzn-s3-demo-bucket"
}
```

有关更多信息，请参阅 Amazon S3 用户指南 ACLs中的控制对象所有权和禁用。

示例 3：在“us-east-1”区域之外创建存储桶

以下 create-bucket 示例在 eu-west-1 区域中创建名为 amzn-s3-demo-bucket 的存储桶。us-east-1 之外的区域需要指定相应的 LocationConstraint 才能在所需区域创建存储桶。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

输出：

```
{
    "Location": "http://amzn-s3-demo-bucket.s3.amazonaws.com/"
}
```

有关更多信息，请参阅《Amazon S3 用户指南》中的创建存储桶。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考CreateBucket中的。

Go

适用于 Go 的 SDK V2

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

使用默认配置创建存储桶。

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
```

```
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(ctx context.Context, name string, region
 string) error {
 _, err := basics.S3Client.CreateBucket(ctx, &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
   log.Printf("You already own bucket %s.\n", name)
   err = owned
  } else if errors.As(err, &exists) {
   log.Printf("Bucket %s already exists.\n", name)
   err = exists
  }
 } else {
  err = s3.NewBucketExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadBucketInput{Bucket: aws.String(name)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for bucket %s to exist.\n", name)
  }
 }
 return err
}
```

创建带有对象锁定功能的存储桶，并等待该存储桶创建成功。

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "log"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// S3Actions wraps S3 service actions.
type S3Actions struct {
 S3Client  *s3.Client
 S3Manager *manager.Uploader
}



// CreateBucketWithLock creates a new S3 bucket with optional object locking
 enabled
// and waits for the bucket to exist before returning.
func (actor S3Actions) CreateBucketWithLock(ctx context.Context, bucket string,
 region string, enableObjectLock bool) (string, error) {
 input := &s3.CreateBucketInput{
  Bucket: aws.String(bucket),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 }

 if enableObjectLock {
  input.ObjectLockEnabledForBucket = aws.Bool(true)
 }

 _, err := actor.S3Client.CreateBucket(ctx, input)
 if err != nil {
  var owned *types.BucketAlreadyOwnedByYou
  var exists *types.BucketAlreadyExists
  if errors.As(err, &owned) {
```

```
    log.Printf("You already own bucket %s.\n", bucket)
    err = owned
   } else if errors.As(err, &exists) {
    log.Printf("Bucket %s already exists.\n", bucket)
    err = exists
   }
  } else {
   err = s3.NewBucketExistsWaiter(actor.S3Client).Wait(
    ctx, &s3.HeadBucketInput{Bucket: aws.String(bucket)}, time.Minute)
   if err != nil {
    log.Printf("Failed attempt to wait for bucket %s to exist.\n", bucket)
   }
  }

  return bucket, err
}
```

- 有关 API 的详细信息，请参阅 适用于 Go 的 Amazon SDK API 参考CreateBucket中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

创建存储桶。

```
    /**
     * Creates an S3 bucket asynchronously.
     *
     * @param bucketName the name of the S3 bucket to create
     * @return a {@link CompletableFuture} that completes when the bucket is
 created and ready
     * @throws RuntimeException if there is a failure while creating the bucket
     */
```

```
   public CompletableFuture<Void> createBucketAsync(String bucketName) {
       CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
           .bucket(bucketName)
           .build();

       CompletableFuture<CreateBucketResponse> response =
getAsyncClient().createBucket(bucketRequest);
       return response.thenCompose(resp -> {
           S3AsyncWaiter s3Waiter = getAsyncClient().waiter();
           HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
               .bucket(bucketName)
               .build();

           CompletableFuture<WaiterResponse<HeadBucketResponse>>
waiterResponseFuture =
               s3Waiter.waitUntilBucketExists(bucketRequestWait);
           return waiterResponseFuture.thenAccept(waiterResponse -> {
               waiterResponse.matched().response().ifPresent(headBucketResponse
-> {
                   logger.info(bucketName + " is ready");
               });
           });
       }).whenComplete((resp, ex) -> {
           if (ex != null) {
               throw new RuntimeException("Failed to create bucket", ex);
           }
       });
   }
```

创建一个启用对象锁定的存储桶。

```
   // Create a new Amazon S3 bucket with object lock options.
   public void createBucketWithLockOptions(boolean enableObjectLock, String
bucketName) {
       S3Waiter s3Waiter = getClient().waiter();
       CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
           .bucket(bucketName)
           .objectLockEnabledForBucket(enableObjectLock)
           .build();

       getClient().createBucket(bucketRequest);
       HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
```

```
            .bucket(bucketName)
            .build();

        // Wait until the bucket is created and print out the response.
        s3Waiter.waitUntilBucketExists(bucketRequestWait);
        System.out.println(bucketName + " is ready");
    }
```

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考CreateBucket中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

创建存储桶。

```
import {
  BucketAlreadyExists,
  BucketAlreadyOwnedByYou,
  CreateBucketCommand,
  S3Client,
  waitUntilBucketExists,
} from "@aws-sdk/client-s3";

/**
 * Create an Amazon S3 bucket.
 * @param {{ bucketName: string }} config
 */
export const main = async ({ bucketName }) => {
  const client = new S3Client({});

  try {
    const { Location } = await client.send(
      new CreateBucketCommand({
```

```
        // The name of the bucket. Bucket names are unique and have several other
 constraints.
        // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
        Bucket: bucketName,
      }),
    );
    await waitUntilBucketExists({ client }, { Bucket: bucketName });
    console.log(`Bucket created with location ${Location}`);
  } catch (caught) {
    if (caught instanceof BucketAlreadyExists) {
      console.error(
        `The bucket "${bucketName}" already exists in another AWS account. Bucket
 names must be globally unique.`,
      );
    }
    // WARNING: If you try to create a bucket in the North Virginia region,
    // and you already own a bucket in that region with the same name, this
    // error will not be thrown. Instead, the call will return successfully
    // and the ACL on that bucket will be reset.
    else if (caught instanceof BucketAlreadyOwnedByYou) {
      console.error(
        `The bucket "${bucketName}" already exists in this AWS account.`,
      );
    } else {
      throw caught;
    }
  }
};
```

- 有关更多信息，请参阅《适用于 JavaScript 的 Amazon SDK 开发人员指南》https://docs.amazonaws.cn/sdk-for-javascript/v3/developer-guide/s3-example-creating-buckets.html#s3-example-creating-buckets-new-bucket-2。
- 有关 API 的详细信息，请参阅 适用于 JavaScript 的 Amazon SDK API 参考CreateBucket中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun createNewBucket(bucketName: String) {
    val request =
        CreateBucketRequest {
            bucket = bucketName
        }

    S3Client.fromEnvironment { region = "us-east-1" }.use { s3 ->
        s3.createBucket(request)
        println("$bucketName is ready")
    }
}
```

- 有关 API 的详细信息，请参阅适用CreateBucket于 K otlin 的Amazon SDK API 参考。

PHP

适用于 PHP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

创建存储桶。

```
        $s3client = new Aws\S3\S3Client(['region' => 'us-west-2']);

        try {
```

```
            $this->s3client->createBucket([
                'Bucket' => $this->bucketName,
                'CreateBucketConfiguration' => ['LocationConstraint' => $region],
            ]);
            echo "Created bucket named: $this->bucketName \n";
        } catch (Exception $exception) {
            echo "Failed to create bucket $this->bucketName with error: " .
 $exception->getMessage();
            exit("Please fix error with bucket creation before continuing.");
        }
```

- 有关 API 的详细信息，请参阅 适用于 PHP 的 Amazon SDK API 参考CreateBucket中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

使用默认设置创建存储桶。

```
class BucketWrapper:
    """Encapsulates S3 bucket actions."""

    def __init__(self, bucket):
        """
        :param bucket: A Boto3 Bucket resource. This is a high-level resource in
 Boto3
                       that wraps bucket actions in a class-like structure.
        """
        self.bucket = bucket
        self.name = bucket.name


    def create(self, region_override=None):
        """
```

```
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

        :param region_override: The Region in which to create the bucket. If this
 is
                                not specified, the Region configured in your
 shared
                                credentials is used.
        """
        if region_override is not None:
            region = region_override
        else:
            region = self.bucket.meta.client.meta.region_name
        try:
            self.bucket.create(CreateBucketConfiguration={"LocationConstraint":
 region})

            self.bucket.wait_until_exists()
            logger.info("Created bucket '%s' in region=%s", self.bucket.name,
 region)
        except ClientError as error:
            logger.exception(
                "Couldn't create bucket named '%s' in region=%s.",
                self.bucket.name,
                region,
            )
            raise error
```

使用生命周期配置创建版本控制的桶。

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.
```

```
    Usage is shown in the usage_demo_single_object function at the end of this
module.

    :param bucket_name: The name of the bucket to create.
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
```

```
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

- 有关 API 的详细信息，请参阅适用CreateBucket于 Python 的Amazon SDK (Boto3) API 参考。

Ruby

适用于 Ruby 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
require 'aws-sdk-s3'

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

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
```

```
  #                                   create is called.
  def initialize(bucket)
    @bucket = bucket
  end

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

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket:
 @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

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

run_demo if $PROGRAM_NAME == __FILE__
```

- 有关 API 的详细信息，请参阅 适用于 Ruby 的 Amazon SDK API 参考CreateBucket中的。

Rust

适用于 Rust 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
pub async fn create_bucket(
    client: &aws_sdk_s3::Client,
    bucket_name: &str,
    region: &aws_config::Region,
) -> Result<Option<aws_sdk_s3::operation::create_bucket::CreateBucketOutput>,
 S3ExampleError> {
    let constraint =
 aws_sdk_s3::types::BucketLocationConstraint::from(region.to_string().as_str());
    let cfg = aws_sdk_s3::types::CreateBucketConfiguration::builder()
        .location_constraint(constraint)
        .build();
    let create = client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await;

    // BucketAlreadyExists and BucketAlreadyOwnedByYou are not problems for this
 task.
    create.map(Some).or_else(|err| {
        if err
            .as_service_error()
            .map(|se| se.is_bucket_already_exists() ||
 se.is_bucket_already_owned_by_you())
            == Some(true)
        {
            Ok(None)
```

```
        } else {
            Err(S3ExampleError::from(err))
        }
    })
}
```

- 有关 API 的详细信息，请参阅适用CreateBucket于 Rust 的Amazon SDK API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    TRY.
        " determine our region from our session
        DATA(lv_region) = CONV /aws1/s3_bucketlocationcnstrnt( lo_session-
>get_region( ) ).
        DATA lo_constraint TYPE REF TO /aws1/cl_s3_createbucketconf.
        " When in the us-east-1 region, you must not specify a constraint
        " In all other regions, specify the region as the constraint
        IF lv_region = 'us-east-1'.
          CLEAR lo_constraint.
        ELSE.
          lo_constraint = NEW /aws1/cl_s3_createbucketconf( lv_region ).
        ENDIF.

        lo_s3->createbucket(
            iv_bucket = iv_bucket_name
            io_createbucketconfiguration  = lo_constraint ).
        MESSAGE 'S3 bucket created.' TYPE 'I'.
      CATCH /aws1/cx_s3_bucketalrdyexists.
        MESSAGE 'Bucket name already exists.' TYPE 'E'.
      CATCH /aws1/cx_s3_bktalrdyownedbyyou.
        MESSAGE 'Bucket already exists and is owned by you.' TYPE 'E'.
    ENDTRY.
```

- 有关 API 的详细信息，请参阅适用CreateBucket于 S AP 的Amazon SDK ABAP API 参考。

Swift

适用于 Swift 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
import AWSS3

    public func createBucket(name: String) async throws {
        var input = CreateBucketInput(
            bucket: name
        )

        // For regions other than "us-east-1", you must set the
 locationConstraint in the createBucketConfiguration.
        // For more information, see LocationConstraint in the S3 API guide.
        // https://docs.aws.amazon.com/AmazonS3/latest/API/
API_CreateBucket.html#API_CreateBucket_RequestBody
        if let region = configuration.region {
            if region != "us-east-1" {
                input.createBucketConfiguration =
 S3ClientTypes.CreateBucketConfiguration(locationConstraint:
 S3ClientTypes.BucketLocationConstraint(rawValue: region))
            }
        }

        do {
            _ = try await client.createBucket(input: input)
        }
        catch let error as BucketAlreadyOwnedByYou {
            print("The bucket '\(name)' already exists and is owned by you. You
 may wish to ignore this exception.")
            throw error
        }
```

```
        catch {
            print("ERROR: ", dump(error, name: "Creating a bucket"))
            throw error
        }
    }
```

- 有关 API 的详细信息，请参阅适用于 S wift 的Amazon SDK API 参考CreateBucket中。

> **Note**
>
> 您也可以使用另一个账户中的 Amazon S3 存储桶，但您可能需要为该存储桶创建策略以便向 Amazon Config授予访问权限。有关向 Amazon S3 存储桶授予权限的信息，请参阅，Amazon Config 传送渠道的 Amazon S3 存储桶的权限然后转至。第 2 步：创建 Amazon SNS 主题

第 2 步：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。步骤 3：创建 IAM 角色

使用 SNS 控制台

创建 Amazon SNS 主题

1. 在 v3/home 上打开亚马逊 SNS 控制台。https://console.aws.amazon.com/sns/
2. 请执行以下操作之一：
   - 如果 Amazon Web Services 账户 之前未在您的主题下创建过任何主题，请阅读主页上对 Amazon SNS 的描述。
   - 如果 Amazon Web Services 账户 之前在您的下方创建过主题，请在导航面板上选择主题。
3. 在 Topics（主页）页面上，选择 Create topic（创建主题）。
4. 在 Create topic（创建主题）页面上，在 Details（详细信息）部分中，执行以下操作：
   a. 对于 Type（类型），选择主题类型（标准或者FIFO）。
   b. 输入主题的名称。对于 FIFO 主题，将 .fifo 添加到名称的末尾。
   c. （可选）输入主题的显示名称。

d. （可选）对于 FIFO 主题，您可以选择基于内容的消息重复数据删除以启用默认的消息重复数据删除。有关更多信息，请参阅 FIFO 主题的消息重复数据删除。

5. （可选）展开加密部分并执行以下操作。有关更多信息，请参阅静态加密。

a. 选择启用加密。

b. 指定客户主密钥（CMK）。有关更多信息，请参阅关键术语。

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

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

- 默认情况下，Amazon SNS 的 Amazon 托管 CMK（默认alias/aws/sns）处于选中状态。

> **Note**
>
> 记住以下内容：
>
> - 首次使用为主题 Amazon KMS 指定适用于 Amazon SNS 的 Amazon 托管 CMK 时，会为 Amazon SNS 创建 Amazon 托管 CMK。 Amazon Web Services 管理控制台
> - 或者，在启用 SSE 的情况下首次对主题使用`Publish`操作时， Amazon KMS 会为 Amazon SNS 创建 Amazon 托管 CMK。

- 要使用您的自定义 CMK Amazon Web Services 账户，请选择客户主密钥 (CMK) 字段，然后从列表中选择自定义 CMK。

> **Note**
>
> 有关创建自定义密钥的说明 CMKs，请参阅《Amazon Key Management Service 开发者指南》中的创建密钥

- 要使用来自 Amazon Web Services 账户 您 Amazon 或其他账户的自定义 CMK ARN，请将其输入到客户主密钥 (CM K) 字段。

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

   > **Note**
   >
   > 使用控制台创建主题时，默认策略使用 `aws:SourceOwner` 条件键。此密钥类似于。`aws:SourceAccount`

7. （可选）要配置 Amazon SNS 重试失败消息传输尝试的方式，请展开 Delivery retry policy（HTTP/S）（传输重试策略（HTTP/S））部分。有关更多信息，请参阅 Amazon SNS 消息传输重试。
8. （可选）要配置 Amazon SNS 如何记录向其发送的消息 CloudWatch，请展开传送状态记录部分。有关更多信息，请参阅 Amazon SNS 消息传输状态。
9. （可选）要将元数据标签添加到主题中，请展开标签部分，输入一个键和值（可选），然后选择添加标签。有关更多信息，请参阅 Amazon SNS 主题标记。
10. 选择创建主题。

    主题已创建并显示***MyTopic***页面。

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

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

使用电子邮件地址订阅 Amazon SNS 主题

1. 在 v3/home 上打开亚马逊 SNS 控制台。https://console.aws.amazon.com/sns/
2. 在左侧导航窗格中，选择订阅。
3. 在订阅页面上，选择创建订阅。
4. 在创建订阅页上的详细信息部分，执行以下操作：

   a. 对于 Topic ARN（主题 ARN），选择主题的 Amazon Resource Name（ARN）。

b. 对于 Protocol（协议），选择终端节点类型。可用的终端节点类型包括：

- HTTP/HTTPS
- 电子邮件/电子邮件-JSON
- Amazon Data Firehose
- Amazon SQS

> **Note**
>
> 要订阅到 SNS FIFO 主题，请选择该选项。

- Amazon Lambda
- 平台应用程序终端节点
- 短信

c. 对于 Endpoint（终端节点），输入终端节点值，例如电子邮件地址或 Amazon SQS 队列的 ARN。

d. 仅限于 Firehose 端点：对于订阅角色 ARN，指定您为写入到 Firehose 传输流创建的 IAM 角色的 ARN。有关更多信息，请参阅订阅 Firehose 传输流到 Amazon SNS 主题的先决条件。

e. （可选）对于 Firehose、Amazon SQS HTTP/S 、终端节点，您还可以启用原始消息传输。有关更多信息，请参阅 Amazon SNS 原始消息传输。

f. （可选）要配置筛选策略，请展开 Subscription filter policy（订阅筛选策略）部分。有关更多信息，请参阅 Amazon SNS 订阅筛选策略。

g. （可选）要为订阅配置死信队列，请展开 Redrive policy（dead-letter queue）（重新驱动策略（死信队列））部分。有关更多信息，请参阅 Amazon SNS 死信队列 ()。DLQs

h. 选择创建订阅。

控制台将创建订阅并打开订阅的 Details（详细信息）页面。

使用 Amazon SDKs

要使用 S Amazon DK，必须使用您的凭据对其进行配置。有关更多信息，请参阅《工具参考指南》和《工具参考指南》中的共享配置Amazon SDKs 和凭据文件。

以下代码示例演示如何使用 `CreateTopic`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

使用特定的名称创建主题。

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

    /// <summary>
    /// This example shows how to use Amazon Simple Notification Service
    /// (Amazon SNS) to add a new Amazon SNS topic.
    /// </summary>
    public class CreateSNSTopic
    {
        public static async Task Main()
        {
            string topicName = "ExampleSNSTopic";

            IAmazonSimpleNotificationService client = new
 AmazonSimpleNotificationServiceClient();

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

        /// <summary>
        /// Creates a new SNS topic using the supplied topic name.
        /// </summary>
        /// <param name="client">The initialized SNS client object used to
        /// create the new topic.</param>
        /// <param name="topicName">A string representing the topic name.</param>
        /// <returns>The Amazon Resource Name (ARN) of the created topic.</
returns>
```

```
        public static async Task<string>
 CreateSNSTopicAsync(IAmazonSimpleNotificationService client, string topicName)
        {
            var request = new CreateTopicRequest
            {
                Name = topicName,
            };

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

创建一个包含名称以及特定 FIFO 和重复数据消除属性的新主题。

```
    /// <summary>
    /// Create a new topic with a name and specific FIFO and de-duplication
 attributes.
    /// </summary>
    /// <param name="topicName">The name for the topic.</param>
    /// <param name="useFifoTopic">True to use a FIFO topic.</param>
    /// <param name="useContentBasedDeduplication">True to use content-based de-
duplication.</param>
    /// <returns>The ARN of the new topic.</returns>
    public async Task<string> CreateTopicWithName(string topicName, bool
 useFifoTopic, bool useContentBasedDeduplication)
    {
        var createTopicRequest = new CreateTopicRequest()
        {
            Name = topicName,
        };

        if (useFifoTopic)
        {
            // Update the name if it is not correct for a FIFO topic.
            if (!topicName.EndsWith(".fifo"))
            {
                createTopicRequest.Name = topicName + ".fifo";
            }
```

```
            // Add the attributes from the method parameters.
            createTopicRequest.Attributes = new Dictionary<string, string>
            {
                { "FifoTopic", "true" }
            };
            if (useContentBasedDeduplication)
            {
                createTopicRequest.Attributes.Add("ContentBasedDeduplication",
 "true");
            }
        }

        var createResponse = await
 _amazonSNSClient.CreateTopicAsync(createTopicRequest);
        return createResponse.TopicArn;
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考CreateTopic中的。

C++

SDK for C++

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
//! Create an Amazon Simple Notification Service (Amazon SNS) topic.
/*!
  \param topicName: An Amazon SNS topic name.
  \param topicARNResult: String to return the Amazon Resource Name (ARN) for the
 topic.
  \param clientConfiguration: AWS client configuration.
  \return bool: Function succeeded.
 */
bool AwsDoc::SNS::createTopic(const Aws::String &topicName,
                              Aws::String &topicARNResult,
                              const Aws::Client::ClientConfiguration
 &clientConfiguration) {
```

```
    Aws::SNS::SNSClient snsClient(clientConfiguration);

    Aws::SNS::Model::CreateTopicRequest request;
    request.SetName(topicName);

    const Aws::SNS::Model::CreateTopicOutcome outcome =
 snsClient.CreateTopic(request);

    if (outcome.IsSuccess()) {
        topicARNResult = outcome.GetResult().GetTopicArn();
        std::cout << "Successfully created an Amazon SNS topic " << topicName
                  << " with topic ARN '" << topicARNResult
                  << "'." << std::endl;

    }
    else {
        std::cerr << "Error creating topic " << topicName << ":" <<
                  outcome.GetError().GetMessage() << std::endl;
        topicARNResult.clear();
    }

    return outcome.IsSuccess();
}
```

- 有关 API 的详细信息，请参阅 适用于 C++ 的 Amazon SDK API 参考CreateTopic中的。

CLI

Amazon CLI

创建 SNS 主题

以下 `create-topic` 示例将创建名为 `my-topic` 的 SNS 主题。

```
aws sns create-topic \
    --name my-topic
```

输出：

```
{
    "ResponseMetadata": {
```

```
        "RequestId": "1469e8d7-1642-564e-b85d-a19b4b341f83"
    },
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:my-topic"
}
```

有关更多信息，请参阅《 Amazon 命令行界面用户指南》中的在 Amazon SQS 和 Amazon SNS 中使用命令Amazon 行界面。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考CreateTopic中的。

Go

适用于 Go 的 SDK V2

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/sns"
 "github.com/aws/aws-sdk-go-v2/service/sns/types"
)

// SnsActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type SnsActions struct {
 SnsClient *sns.Client
}



// CreateTopic creates an Amazon SNS topic with the specified name. You can
 optionally
```

```
// specify that the topic is created as a FIFO topic and whether it uses content-
based
// deduplication instead of ID-based deduplication.
func (actor SnsActions) CreateTopic(ctx context.Context, topicName string,
 isFifoTopic bool, contentBasedDeduplication bool) (string, error) {
 var topicArn string
 topicAttributes := map[string]string{}
 if isFifoTopic {
  topicAttributes["FifoTopic"] = "true"
 }
 if contentBasedDeduplication {
  topicAttributes["ContentBasedDeduplication"] = "true"
 }
 topic, err := actor.SnsClient.CreateTopic(ctx, &sns.CreateTopicInput{
  Name:       aws.String(topicName),
  Attributes: topicAttributes,
 })
 if err != nil {
  log.Printf("Couldn't create topic %v. Here's why: %v\n", topicName, err)
 } else {
  topicArn = *topic.TopicArn
 }

 return topicArn, err
}
```

- 有关 API 的详细信息，请参阅 适用于 Go 的 Amazon SDK API 参考CreateTopic中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.sns.SnsClient;
```

```
import software.amazon.awssdk.services.sns.model.CreateTopicRequest;
import software.amazon.awssdk.services.sns.model.CreateTopicResponse;
import software.amazon.awssdk.services.sns.model.SnsException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class CreateTopic {
    public static void main(String[] args) {
        final String usage = """

                Usage:    <topicName>

                Where:
                   topicName - The name of the topic to create (for example,
 mytopic).

                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String topicName = args[0];
        System.out.println("Creating a topic with name: " + topicName);
        SnsClient snsClient = SnsClient.builder()
                .region(Region.US_EAST_1)
                .build();

        String arnVal = createSNSTopic(snsClient, topicName);
        System.out.println("The topic ARN is" + arnVal);
        snsClient.close();
    }

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
```

```
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

            result = snsClient.createTopic(request);
            return result.topicArn();

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

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考CreateTopic中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库 中查找完整示例，了解如何进行设置和运行。

在单独的模块中创建客户端并将其导出。

```
import { SNSClient } from "@aws-sdk/client-sns";

// The AWS Region can be provided here using the `region` property. If you leave
 it blank
// the SDK will default to the region set in your AWS config.
export const snsClient = new SNSClient({});
```

导入 SDK 和客户端模块，然后调用 API。

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
```

```
import { snsClient } from "../libs/snsClient.js";

/**
 * @param {string} topicName - The name of the topic to create.
 */
export const createTopic = async (topicName = "TOPIC_NAME") => {
  const response = await snsClient.send(
    new CreateTopicCommand({ Name: topicName }),
  );
  console.log(response);
  // {
  //   '$metadata': {
  //     httpStatusCode: 200,
  //     requestId: '087b8ad2-4593-50c4-a496-d7e90b82cf3e',
  //     extendedRequestId: undefined,
  //     cfId: undefined,
  //     attempts: 1,
  //     totalRetryDelay: 0
  //   },
  //   TopicArn: 'arn:aws:sns:us-east-1:xxxxxxxxxxxx:TOPIC_NAME'
  // }
  return response;
};
```

- 有关更多信息，请参阅《适用于 JavaScript 的 Amazon SDK Developer Guide》。
- 有关 API 的详细信息，请参阅 适用于 JavaScript 的 Amazon SDK API 参考CreateTopic中的。

Kotlin

适用于 Kotlin 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
suspend fun createSNSTopic(topicName: String): String {
    val request =
```

```
        CreateTopicRequest {
            name = topicName
        }

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

- 有关 API 的详细信息，请参阅适用CreateTopic于 K otlin 的Amazon SDK API 参考。

PHP

适用于 PHP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

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

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


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

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

```
]);

$topicname = 'myTopic';

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

- 有关更多信息，请参阅《适用于 PHP 的 Amazon SDK 开发人员指南》https://docs.amazonaws.cn/sdk-for-php/v3/developer-guide/sns-examples-managing-topics.html#create-a-topic。
- 有关 API 的详细信息，请参阅 适用于 PHP 的 Amazon SDK API 参考CreateTopic中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class SnsWrapper:
    """Encapsulates Amazon SNS topic and subscription functions."""

    def __init__(self, sns_resource):
        """
        :param sns_resource: A Boto3 Amazon SNS resource.
        """
        self.sns_resource = sns_resource
```

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

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

```
class SnsWrapper:
    """Wrapper class for managing Amazon SNS operations."""

    def __init__(self, sns_client: Any) -> None:
        """
        Initialize the SnsWrapper.

        :param sns_client: A Boto3 Amazon SNS client.
        """
        self.sns_client = sns_client

    @classmethod
    def from_client(cls) -> 'SnsWrapper':
        """
        Create an SnsWrapper instance using a default boto3 client.

        :return: An instance of this class.
        """
        sns_client = boto3.client('sns')
        return cls(sns_client)


    def create_topic(
        self,
        topic_name: str,
```

```
        is_fifo: bool = False,
        content_based_deduplication: bool = False
    ) -> str:
        """
        Create an SNS topic.

        :param topic_name: The name of the topic to create.
        :param is_fifo: Whether to create a FIFO topic.
        :param content_based_deduplication: Whether to use content-based
deduplication for FIFO topics.
        :return: The ARN of the created topic.
        :raises ClientError: If the topic creation fails.
        """
        try:
            # Add .fifo suffix for FIFO topics
            if is_fifo and not topic_name.endswith('.fifo'):
                topic_name += '.fifo'

            attributes = {}
            if is_fifo:
                attributes['FifoTopic'] = 'true'
                if content_based_deduplication:
                    attributes['ContentBasedDeduplication'] = 'true'

            response = self.sns_client.create_topic(
                Name=topic_name,
                Attributes=attributes
            )

            topic_arn = response['TopicArn']
            logger.info(f"Created topic: {topic_name} with ARN: {topic_arn}")
            return topic_arn

        except ClientError as e:
            error_code = e.response.get('Error', {}).get('Code', 'Unknown')
            logger.error(f"Error creating topic {topic_name}: {error_code} -
{e}")
            raise
```

- 有关 API 的详细信息，请参阅适用CreateTopic于 Python 的Amazon SDK (Boto3) API 参考。

Ruby

适用于 Ruby 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
# This class demonstrates how to create an Amazon Simple Notification Service
 (SNS) topic.
class SNSTopicCreator
  # Initializes an SNS client.
  #
  # Utilizes the default AWS configuration for region and credentials.
  def initialize
    @sns_client = Aws::SNS::Client.new
  end

  # Attempts to create an SNS topic with the specified name.
  #
  # @param topic_name [String] The name of the SNS topic to create.
  # @return [Boolean] true if the topic was successfully created, false
 otherwise.
  def create_topic(topic_name)
    @sns_client.create_topic(name: topic_name)
    puts "The topic '#{topic_name}' was successfully created."
    true
  rescue Aws::SNS::Errors::ServiceError => e
    # Handles SNS service errors gracefully.
    puts "Error while creating the topic named '#{topic_name}': #{e.message}"
    false
  end
end

# Example usage:
if $PROGRAM_NAME == __FILE__
  topic_name = 'YourTopicName' # Replace with your topic name
  sns_topic_creator = SNSTopicCreator.new

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

```
  unless sns_topic_creator.create_topic(topic_name)
    puts 'The topic was not created. Stopping program.'
    exit 1
  end
end
```

- 有关更多信息，请参阅《适用于 Ruby 的 Amazon SDK 开发人员指南》https://docs.amazonaws.cn/sdk-for-ruby/v3/developer-guide/sns-example-create-topic.html。
- 有关 API 的详细信息，请参阅 适用于 Ruby 的 Amazon SDK API 参考CreateTopic中的。

Rust

适用于 Rust 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

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

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

    Ok(())
}
```

- 有关 API 的详细信息，请参阅适用CreateTopic于 Rust 的Amazon SDK API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
   TRY.
       oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
is returned for testing purposes. "
       MESSAGE 'SNS topic created' TYPE 'I'.
     CATCH /aws1/cx_snstopiclimitexcdex.
       MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

- 有关 API 的详细信息，请参阅适用CreateTopic于 S AP 的Amazon SDK ABAP API 参考。

Swift

适用于 Swift 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
import AWSSNS

        let config = try await SNSClient.SNSClientConfiguration(region: region)
        let snsClient = SNSClient(config: config)

        let output = try await snsClient.createTopic(
            input: CreateTopicInput(name: name)
        )
```

```
        guard let arn = output.topicArn else {
            print("No topic ARN returned by Amazon SNS.")
            return
        }
```

- 有关 API 的详细信息，请参阅适用于 S wift 的Amazon SDK API 参考CreateTopic中。

> **Note**
>
> 您也可以使用另一个账户中的 Amazon SNS 主题，但在这种情况下，您可能需要为该主题创建策略以便向 Amazon Config授予访问权限。有关向 Amazon SNS 主题授予访问权限的信息，请参阅，Amazon SNS 主题的权限然后转至。步骤 3：创建 IAM 角色

步骤 3：创建 IAM 角色

> **Important**
>
> （推荐）使用 Amazon Config 服务相关角色
> 建议使用 Amazon Config 服务相关角色:`AWSServiceRoleForConfig`。服务相关角色是预定义的，包括调用其他 Amazon Web Services 服务角色 Amazon Config 所需的所有权限。与 Amazon Config 服务相关的配置记录器需要服务相关角色。
> 有关更多信息，请参阅为 Amazon Config使用服务相关角色。

使用 IAM 控制台

您可以使用 IAM 控制台创建一个 IAM 角色，该角色授予访问您的 Amazon S3 存储桶、访问您的 Amazon SNS 主题以及获取支持 Amazon 资源的配置详细信息的 Amazon Config 权限。当您使用控制台创建 IAM 角色时， Amazon Config 会自动为您将必需权限附加到该角色。

> **Note**
>
> 如果您使用的是使用的 Amazon 服务 Amazon Config （例如 Sec Amazon urity Hub 或 Cont Amazon rol Tower），并且已经创建了角色，则应确保在设置时使用的 IAM 角色与已创建的 Amazon Config 角色 Amazon Config 保持相同的最低权限，以便其他 Amazon 服务继续按预期运行。 Amazon Config

例如，如果 Cont Amazon rol Tower 有一个 Amazon Config 允许读取 Amazon S3 对象的 IAM 角色，则应保证在设置时使用的 IAM 角色中授予的权限相同 Amazon Config。否则，它可能会干扰 Amazon 控制塔的运行。
有关的 IAM 角色的更多信息 Amazon Config，请参阅 Ident Amazon ity and Access 管理。

为 Amazon 服务创建角色

1. 登录 Amazon Web Services 管理控制台 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
3. 对于选择可信实体，选择 Amazon 服务。
4. 选择你想要的用例 Amazon Config：Config-可自定义、Config-Organizations、Con fig 或 Config-Conformance Packs。然后选择下一步。
5. 在命名、查看和创建页面上，查看有关您的角色的详细信息，然后选择创建角色。

使用 Amazon SDKs

要使用 S Amazon DK，必须使用您的凭据对其进行配置。有关更多信息，请参阅《工具参考指南》和《工具参考指南》中的共享配置Amazon SDKs 和凭据文件。

以下代码示例演示如何使用 `CreateRole`。

.NET

适用于 .NET 的 Amazon SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
/// <summary>
/// Create a new IAM role.
/// </summary>
/// <param name="roleName">The name of the IAM role.</param>
/// <param name="rolePolicyDocument">The name of the IAM policy document
```

```
    /// for the new role.</param>
    /// <returns>The Amazon Resource Name (ARN) of the role.</returns>
    public async Task<string> CreateRoleAsync(string roleName, string
 rolePolicyDocument)
    {
        var request = new CreateRoleRequest
        {
            RoleName = roleName,
            AssumeRolePolicyDocument = rolePolicyDocument,
        };

        var response = await _IAMService.CreateRoleAsync(request);
        return response.Role.Arn;
    }
```

- 有关 API 的详细信息，请参阅 适用于 .NET 的 Amazon SDK API 参考CreateRole中的。

Bash

Amazon CLI 使用 Bash 脚本

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
#####################################################################################
# function errecho
#
# This function outputs everything sent to it to STDERR (standard error output).
#####################################################################################
function errecho() {
  printf "%s\n" "$*" 1>&2
}

#####################################################################################
# function iam_create_role
#
# This function creates an IAM role.
```

```
#
# Parameters:
#       -n role_name -- The name of the IAM role.
#       -p policy_json -- The assume role policy document.
#
# Returns:
#       The ARN of the role.
#     And:
#       0 - If successful.
#       1 - If it fails.
###############################################################################
function iam_create_role() {
  local role_name policy_document response
  local option OPTARG # Required to use getopts command in a function.

  # bashsupport disable=BP5008
  function usage() {
    echo "function iam_create_user_access_key"
    echo "Creates an AWS Identity and Access Management (IAM) role."
    echo "  -n role_name   The name of the IAM role."
    echo "  -p policy_json -- The assume role policy document."
    echo ""
  }

  # Retrieve the calling parameters.
  while getopts "n:p:h" option; do
    case "${option}" in
      n) role_name="${OPTARG}" ;;
      p) policy_document="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done
  export OPTIND=1

  if [[ -z "$role_name" ]]; then
    errecho "ERROR: You must provide a role name with the -n parameter."
```

```
    usage
    return 1
  fi

  if [[ -z "$policy_document" ]]; then
    errecho "ERROR: You must provide a policy document with the -p parameter."
    usage
    return 1
  fi

  response=$(aws iam create-role \
    --role-name "$role_name" \
    --assume-role-policy-document "$policy_document" \
    --output text \
    --query Role.Arn)

  local error_code=${?}

  if [[ $error_code -ne 0 ]]; then
    aws_cli_error_log $error_code
    errecho "ERROR: AWS reports create-role operation failed.\n$response"
    return 1
  fi

  echo "$response"

  return 0
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考CreateRole中的。

C++

SDK for C++

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
bool AwsDoc::IAM::createIamRole(
        const Aws::String &roleName,
        const Aws::String &policy,
        const Aws::Client::ClientConfiguration &clientConfig) {
    Aws::IAM::IAMClient client(clientConfig);
    Aws::IAM::Model::CreateRoleRequest request;

    request.SetRoleName(roleName);
    request.SetAssumeRolePolicyDocument(policy);

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- 有关 API 的详细信息，请参阅 适用于 C++ 的 Amazon SDK API 参考CreateRole中的。

CLI

Amazon CLI

示例 1：创建 IAM 角色

以下 `create-role` 命令创建一个名为 `Test-Role` 的角色并对其附加信任策略。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json
```

输出：

```
{
    "Role": {
        "AssumeRolePolicyDocument": "<URL-encoded-JSON>",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "CreateDate": "2013-06-07T20:43:32.821Z",
        "RoleName": "Test-Role",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role"
    }
}
```

信任策略在 Test-Role-Trust-Policy.json 文件中定义为 JSON 文档。（文件名和扩展名没有意义。）信任策略必须指定主体。

要将权限策略附加到角色，请使用 `put-role-policy` 命令。

有关更多信息，请参阅《Amazon IAM 用户指南》中的创建 IAM 角色。

示例 2：创建具有指定最长会话持续时间的 IAM 角色

以下 `create-role` 命令创建一个名为 `Test-Role` 的角色，并将最长会话持续时间设置为 7200 秒（2 小时）。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --max-session-duration 7200
```

输出：

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::12345678012:role/Test-Role",
        "CreateDate": "2023-05-24T23:50:25+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
```

```
                    "Principal": {
                        "AWS": "arn:aws:iam::12345678012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

有关更多信息，请参阅 I Amazon AM 用户指南中的修改角色最长会话持续时间 (Amazon API)。

示例 3：创建带有标签的 IAM 角色

以下命令创建带有标签的 IAM 角色。Test-Role此示例使用带有以下 JSON 格式标签的 --tags 参数标志：'{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location", "Value": "Seattle"}'。或者，--tags 标志可与简写格式的标签一起使用：'Key=Department,Value=Accounting Key=Location,Value=Seattle'。

```
aws iam create-role \
    --role-name Test-Role \
    --assume-role-policy-document file://Test-Role-Trust-Policy.json \
    --tags '{"Key": "Department", "Value": "Accounting"}' '{"Key": "Location",
 "Value": "Seattle"}'
```

输出：

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version":"2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
```

```
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
        ]
    }
}
```

有关更多信息，请参阅《Amazon IAM 用户指南》中的标记 IAM 角色。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考CreateRole中的。

Go

适用于 Go 的 SDK V2

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
import (
 "context"
 "encoding/json"
 "log"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/iam"
 "github.com/aws/aws-sdk-go-v2/service/iam/types"
```

```
)

// RoleWrapper encapsulates AWS Identity and Access Management (IAM) role actions
// used in the examples.
// It contains an IAM service client that is used to perform role actions.
type RoleWrapper struct {
 IamClient *iam.Client
}



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(ctx context.Context, roleName string,
 trustedUserArn string) (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version: "2012-10-17",
  Statement: []PolicyStatement{{
   Effect:    "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
   Action:    []string{"sts:AssumeRole"},
  }},
 }
 policyBytes, err := json.Marshal(trustPolicy)
 if err != nil {
  log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
 trustedUserArn, err)
  return nil, err
 }
 result, err := wrapper.IamClient.CreateRole(ctx, &iam.CreateRoleInput{
  AssumeRolePolicyDocument: aws.String(string(policyBytes)),
  RoleName:                 aws.String(roleName),
 })
 if err != nil {
  log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
 } else {
  role = result.Role
 }
 return role, err
```

```
}
```

- 有关 API 的详细信息，请参阅 适用于 Go 的 Amazon SDK API 参考CreateRole中的。

Java

适用于 Java 的 SDK 2.x

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
import org.json.simple.JSONObject;
import org.json.simple.parser.JSONParser;
import software.amazon.awssdk.services.iam.model.CreateRoleRequest;
import software.amazon.awssdk.services.iam.model.CreateRoleResponse;
import software.amazon.awssdk.services.iam.model.IamException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

/*
*   This example requires a trust policy document. For more information, see:
*   https://aws.amazon.com/blogs/security/how-to-use-trust-policies-with-iam-
roles/
*
*
*  In addition, set up your development environment, including your credentials.
*
*  For information, see this documentation topic:
*
*  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
```

```
                Usage:
                    <rolename> <fileLocation>\s

                Where:
                    rolename - The name of the role to create.\s
                    fileLocation - The location of the JSON document that
represents the trust policy.\s
                """;

        if (args.length != 2) {
            System.out.println(usage);
            System.exit(1);
        }

        String rolename = args[0];
        String fileLocation = args[1];
        Region region = Region.AWS_GLOBAL;
        IamClient iam = IamClient.builder()
                .region(region)
                .build();

        String result = createIAMRole(iam, rolename, fileLocation);
        System.out.println("Successfully created user: " + result);
        iam.close();
    }

    public static String createIAMRole(IamClient iam, String rolename, String
fileLocation) throws Exception {
        try {
            JSONObject jsonObject = (JSONObject)
readJsonSimpleDemo(fileLocation);
            CreateRoleRequest request = CreateRoleRequest.builder()
                    .roleName(rolename)
                    .assumeRolePolicyDocument(jsonObject.toJSONString())
                    .description("Created using the AWS SDK for Java")
                    .build();

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

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

```
        }
        return "";
    }

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

- 有关 API 的详细信息，请参阅 Amazon SDK for Java 2.x API 参考CreateRole中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

创建角色。

```
import { CreateRoleCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
```

```
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
      ],
    }),
    RoleName: roleName,
  });

  return client.send(command);
};
```

- 有关 API 的详细信息，请参阅 适用于 JavaScript 的 Amazon SDK API 参考CreateRole中的。

PHP

适用于 PHP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

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

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

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

- 有关 API 的详细信息，请参阅 适用于 PHP 的 Amazon SDK API 参考CreateRole中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例创建一个名为 **MyNewRole** 的新角色，并将文件 **NewRoleTrustPolicy.json** 中的策略附加到该角色。请注意，必须使用 **-Raw** 开关参数才能成功处理 JSON 策略文件。输出中显示的策略文档采用 URL 编码。在本例中，使用 **UrlDecode** .NET 方法对其进行解码。

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

输出：

```
Arn                       : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                             %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
```

```
                            %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                            %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                            %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                            %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                            %20%5D%0D%0A%7D
CreateDate               : 4/15/2015 11:04:23 AM
Path                     : /
RoleId                   : V5PAJI2KPN4EAEXAMPLE1
RoleName                 : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) CreateRole中的。

适用于 PowerShell V5 的工具

示例 1：此示例创建一个名为 **MyNewRole** 的新角色，并将文件 **NewRoleTrustPolicy.json** 中的策略附加到该角色。请注意，必须使用 **-Raw** 开关参数才能成功处理 JSON 策略文件。输出中显示的策略文档采用 URL 编码。在本例中，使用 **UrlDecode** .NET 方法对其进行解码。

```
$results = New-IAMRole -AssumeRolePolicyDocument (Get-Content -raw
 NewRoleTrustPolicy.json) -RoleName MyNewRole
$results
```

输出：

```
Arn                       : arn:aws:iam::123456789012:role/MyNewRole
AssumeRolePolicyDocument : %7B%0D%0A%20%20%22Version%22%3A%20%222012-10-17%22%2C
%0D%0A%20%20%22Statement%22
                           %3A%20%5B%0D%0A%20%20%20%20%7B%0D%0A
%20%20%20%20%20%20%22Sid%22%3A%20%22%22%2C
                           %0D%0A%20%20%20%20%20%20%22Effect%22%3A%20%22Allow
%22%2C%0D%0A%20%20%20%20%20%20
                           %22Principal%22%3A%20%7B%0D%0A
%20%20%20%20%20%20%20%20%22AWS%22%3A%20%22arn%3Aaws
                           %3Aiam%3A%3A123456789012%3ADavid%22%0D%0A
%20%20%20%20%20%20%7D%2C%0D%0A%20%20%20
                           %20%20%20%22Action%22%3A%20%22sts%3AAssumeRole%22%0D
%0A%20%20%20%20%7D%0D%0A%20
                           %20%5D%0D%0A%7D
CreateDate                : 4/15/2015 11:04:23 AM
Path                      : /
RoleId                    : V5PAJI2KPN4EAEXAMPLE1
RoleName                  : MyNewRole

[System.Reflection.Assembly]::LoadWithPartialName("System.Web.HttpUtility")
[System.Web.HttpUtility]::UrlDecode($results.AssumeRolePolicyDocument)
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:David"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) CreateRole中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

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

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

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

- 有关 API 的详细信息，请参阅适用CreateRole于 Python 的Amazon SDK (Boto3) API 参考。

Ruby

适用于 Ruby 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
 # Creates a role and attaches policies to it.
 #
 # @param role_name [String] The name of the role.
 # @param assume_role_policy_document [Hash] The trust relationship policy
document.
 # @param policy_arns [Array<String>] The ARNs of the policies to attach.
 # @return [String, nil] The ARN of the new role if successful, or nil if an
error occurred.
 def create_role(role_name, assume_role_policy_document, policy_arns)
   response = @iam_client.create_role(
     role_name: role_name,
     assume_role_policy_document: assume_role_policy_document.to_json
   )
   role_arn = response.role.arn

   policy_arns.each do |policy_arn|
     @iam_client.attach_role_policy(
       role_name: role_name,
       policy_arn: policy_arn
     )
   end

   role_arn
 rescue Aws::IAM::Errors::ServiceError => e
   @logger.error("Error creating role: #{e.message}")
   nil
 end
```

- 有关 API 的详细信息，请参阅 适用于 Ruby 的 Amazon SDK API 参考CreateRole中的。

Rust

适用于 Rust 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

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

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

- 有关 API 的详细信息，请参阅适用CreateRole于 Rust 的Amazon SDK API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    TRY.
        oo_result = lo_iam->createrole(
          iv_rolename = iv_role_name
          iv_assumerolepolicydocument = iv_assume_role_policy_document ).
        MESSAGE 'Role created successfully.' TYPE 'I'.
      CATCH /aws1/cx_iamentityalrdyexex.
        MESSAGE 'Role already exists.' TYPE 'E'.
      CATCH /aws1/cx_iammalformedplydocex.
        MESSAGE 'Assume role policy document is malformed.' TYPE 'E'.
      CATCH /aws1/cx_iamlimitexceededex.
        MESSAGE 'Role limit exceeded.' TYPE 'E'.
    ENDTRY.
```

- 有关 API 的详细信息，请参阅适用CreateRole于 S AP 的Amazon SDK ABAP API 参考。

Swift

适用于 Swift 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
import AWSIAM
import AWSS3
```

```
    public func createRole(name: String, policyDocument: String) async throws ->
String {
        let input = CreateRoleInput(
            assumeRolePolicyDocument: policyDocument,
            roleName: name
        )
        do {
            let output = try await client.createRole(input: input)
            guard let role = output.role else {
                throw ServiceHandlerError.noSuchRole
            }
            guard let id = role.roleId else {
                throw ServiceHandlerError.noSuchRole
            }
            return id
        } catch {
            print("ERROR: createRole:", dump(error))
            throw error
        }
    }
```

- 有关 API 的详细信息，请参阅适用于 S wift 的Amazon SDK API 参考CreateRole中。

通过 Amazon CLI 使用客户管理的配置记录器启动 Amazon Config

您可以通过创建客户管理的配置记录器来启动。Amazon Config要使用 Amazon CLI 创建客户管理的配置记录器，请使用以下命令：put-configuration-recorder、put-delivery-channel 和 start-configuration-recorder。

- put-configuration-recorder 命令可创建客户管理的配置记录器。
- put-delivery-channel 命令可创建传输通道，Amazon Config 通过该通道将配置信息传输到 S3 存储桶和 SNS 主题。
- start-configuration-recorder 将启动客户管理的配置记录器。客户管理的配置记录器将开始记录您指定的资源类型的配置更改。

主题

- 注意事项
- 步骤 1：运行 put-configuration-recorder 命令

- 步骤 2：运行 put-delivery-channel 命令
- 步骤 3：运行 start-configuration-recorder 命令

注意事项

S3 存储桶、SNS 主题和 IAM 角色为必填项

要创建客户管理的配置记录器，您需要创建一个 S3 存储桶、一个 SNS 主题和一个具有附加策略的 IAM 角色作为先决条件。要设置 Amazon Config 的先决条件，请参阅先决条件。

每个区域的每个账户配有一个客户管理的配置记录器

每个 Amazon Web Services 区域每个 Amazon Web Services 账户只能有一个客户管理的配置记录器。

每个区域的每个账户配有一个传输通道

每个 Amazon Web Services 区域每个 Amazon Web Services 账户只能有一个传输通道区域。

策略与合规结果

IAM 策略和 Amazon Organizations 中管理的其他策略可能会影响 Amazon Config 是否有权记录资源的配置更改。此外，规则会直接评估资源的配置，且执行评估时不会考虑这些策略。确保现行策略与您打算使用 Amazon Config 的方式保持一致。

步骤 1：运行 put-configuration-recorder 命令

使用 `put-configuration-recorder` 命令创建客户管理的配置记录器：

此命令使用 `--configuration-recorder` 和 `---recording-group` 字段。

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

`configuration-recorder` 字段

`configurationRecorder.json` 文件指定配置记录器的 `name` 和 `roleArn` 以及默认记录频率（`recordingMode`）。您也可以使用此字段来覆盖特定资源类型的记录频率。

```
{
  "name": "default",
```

```
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in the
 override ]
        }
    ]
  }
}
```

recording-group 字段

recordingGroup.json 文件指定要记录哪些资源类型。

```
{
    "allSupported": boolean,
    "exclusionByResourceTypes": {
        "resourceTypes": [ Comma-separated list of resource types to exclude ]
    },
    "includeGlobalResourceTypes": boolean,
    "recordingStrategy": {
        "useOnly": "Recording strategy for the configuration recorder"
    },
    "resourceTypes": [ Comma-separated list of resource types to include]
}
```

有关这些字段的更多信息，请参阅《Amazon CLI 命令参考》中的 put-configuration-recorder

步骤 2：运行 put-delivery-channel 命令

使用 put-delivery-channel 命令创建传输通道：

此命令使用 --delivery-channel 字段。

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

delivery-channel 字段

deliveryChannel.json 文件指定以下内容：

- 传输通道的 name
- s3BucketName：Amazon Config 发送配置快照的地方。
- snsTopicARN：Amazon Config 发送通知的地点
- configSnapshotDeliveryProperties：用于设置 Amazon Config 传输配置快照的频率以及它为定期规则调用评估的频率。

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

有关这些字段的更多信息，请参阅《Amazon CLI 命令参考》中的 put-delivery-channel

步骤 3：运行 start-configuration-recorder 命令

使用 start-configuration-recorder 命令启动 Amazon Config：

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

有关这些字段的更多信息，请参阅《Amazon CLI 命令参考》中的 start-configuration-recorder

验证是否已使用 Amazon CLI 成功启动 Amazon Config

启动 Amazon Config 后，您可以使用 Amazon CLI 命令检查 Amazon Config 是否正在运行，以及 Amazon Config 是否已创建配置记录器和传输渠道。您也可以确认 Amazon Config 是否已开始记录配置并向传递通道传递这些配置。

主题

- 步骤 1：检查是否已创建传输通道
- 步骤 2：检查是否已创建配置记录器
- 步骤 3：检查 Amazon Config 是否已开始记录

步骤 1：检查是否已创建传输通道

使用 describe-delivery-channels 命令检查是否已配置 Amazon S3 存储桶和 Amazon SNS 主题。

您可以使用 --delivery-channel-names 字段来指定传输通道列表。如果未指定传输通道，则此命令将返回与该账户关联的所有传输通道的详细信息。

```
$ 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"
        }
    ]
}
```

步骤 2：检查是否已创建配置记录器

使用 describe-configuration-recorders 命令检查配置记录器是否已创建。

您可以使用 arn 和 configuration-recorder-names 字段来指定配置记录器列表。如果未指定配置记录器，则此命令将返回与该账户关联的所有配置记录器的详细信息。

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

步骤 3：检查 Amazon Config 是否已开始记录

使用 describe-configuration-recorder-status 命令检查配置记录器是否成功记录了范围内的资源类型。

您可以使用 arn 和 configuration-recorder-names 字段来指定配置记录器列表。如果未指定配置记录器，则此命令将返回与该账户关联的所有配置记录器的详细信息。

```
$ 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 true 值用于确认配置记录器已开始记录配置。Amazon Config 采用 UTC 格式来记录时间。输出显示为 Unix 时间戳。

Amazon Config与Amazon SDK 一起使用

Amazon软件开发套件 (SDKs) 可用于许多流行的编程语言。每个软件开发工具包都提供 API、代码示例和文档，使开发人员能够更轻松地以其首选语言构建应用程序。

SDK 文档
Amazon CLI
适用于 Java 的 Amazon SDK
适用于 JavaScript 的 Amazon SDK
适用于 .NET 的 Amazon SDK
适用于 PHP 的 Amazon SDK
Amazon Tools for PowerShell

SDK 文档
适用于 Python (Boto3) 的 Amazon SDK
适用于 Ruby 的 Amazon SDK
适用于 SAP ABAP 的 Amazon SDK

使用配置记录器

配置记录器将范围内资源类型的配置更改存储为配置项目 (CIs)。

有两种类型的配置记录器。

Type	描述
客户管理的配置记录器	您管理的配置记录器。范围内的资源类型由您设置。默认情况下，客户管理的配置记录器会在运行Amazon Web Services 区域位置Amazon Config中记录所有支持的资源。
服务相关配置记录器	链接到特定的配置记录器Amazon Web Services服务。范围内的资源类型由相关服务设置。

主题

- 客户管理的配置记录器的注意事项
- 服务相关配置记录器的注意事项
- 配置记录器的偏离检测
- 启动客户管理的配置记录器
- 停止客户管理的配置记录器
- 更改客户管理的配置记录器的记录频率
- 重命名客户管理的配置记录器
- 查看配置记录器
- 删除配置记录器

客户管理的配置记录器的注意事项

每个区域的每个账户配有一个客户管理的配置记录器

每Amazon Web Services 账户台只能有一个客户管理的配置记录器Amazon Web Services 区域。

默认设置为记录所有支持的资源类型，不包括全局 IAM 资源类型

客户管理的配置记录器的默认设置是记录所有支持的资源类型，不包括以下全局 IAM 资源类型：`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role` 和 `AWS::IAM::User`。您可以指定要在记录范围中包含或排除哪些资源类型。

有关更多信息，请参阅 使用 Amazon Config 记录 Amazon 资源

使用客户管理的配置记录器需要支付服务使用费

Amazon Config开始使用客户管理的配置记录器记录配置时，您需要支付服务使用费。

有关定价信息，请参阅 Amazon Config定价。

Amazon Systems Manager用于在整个组织中创建客户托管的配置记录器

您可以使用Amazon Systems Manager Quick Setup 在多个组织部门 (OUs) 中创建客户托管的配置记录器，并Amazon Web Services 区域使用Amazon最佳实践。

有关更多信息，请参阅《Systems Manager 用户指南》中的 “使用快速设置创建Amazon Config配置记录器”。

> **Important**
>
> 策略与合规结果
> 在中管理@@ 的 IAM 策略和其他策略Amazon Organizations可能会影响您是否Amazon Config有权记录资源的配置更改。此外，规则会直接评估资源的配置，且执行评估时不会考虑这些策略。确保现行策略与您打算使用Amazon Config的方式保持一致。
> 如果配置记录器关闭，已删除资源的状态评估结果可能会持续显示
> 如果客户管理的配置记录器关闭，将会禁用Amazon Config Config 跟踪您指定的资源配置更改的功能，包括其删除操作。这意味着您可能会看到关闭客户托管配置记录器时删除的资源的评估结果过时，因为如果未开启录制，则Amazon Config无法捕获删除事件。

服务相关配置记录器的注意事项

必须使用Amazon Config服务相关角色

与Amazon Config服务相关的配置记录器需要服务相关角色。

有关更多信息，请参阅为Amazon Config使用服务相关角色。

服务相关配置记录器始终处于记录状态

服务相关记录器已修复。您无法直接更改服务相关记录器中的设置。要修改录制器设置，例如启动、停止或更新录制器，请通过使用Amazon服务关联录制器的关联服务进行这些更改。

有关更多信息，请参阅删除配置记录器。

记录范围决定您是否会收到配置项

录制范围由链接到配置记录器的设置Amazon Web Services 服务，并决定您是否在传送渠道中接收配置项目 (CIs)。如果录制范围是内部的，则您不会在配送渠道 CIs 中接收。

记录范围决定是否向您收取服务费

录制范围由链接到配置记录器的设置Amazon Web Services 服务，它决定范围内的配置项目 (CIs) 是免费录制（内部）还是会影响账单成本（已付费）。

记录器之间的记录频率优先级

如果您同时拥有客户管理的配置记录器和记录范围为“PAID”的服务相关配置记录器，并且它们记录相同的资源类型，则记录频率较高的记录器优先。例如，如果您的客户管理的录音机设置为每日录制，但您启用了一项Amazon服务，该服务使用录制范围为 “付费” 且持续录制的服务关联录制器，则将持续录制受影响的资源类型。

这意味着，即使您的客户管理的记录器设置仍显示“每日记录”，但对于同时位于这两个记录器范围内的资源类型，您仍需要支付连续记录费用。这只会影响两个记录器正在记录的资源类型。

> **Note**
>
> 无论客户管理的配置记录器或您付费的服务相关配置记录器生成多少个配置项，每个配置项仅计费一次。

Example 示例：记录频率优先级

您已将客户托管录制器配置为以每日记录频率记录亚马逊 EC2 实例。稍后，您可以启用一项Amazon服务功能，该功能使用记录范围为 “付费” 的服务关联录制器和同时记录 Amazon EC2 实例的连续录制。在此场景中：

- 您的客户管理的记录器设置仍将显示“每日记录”
- Amazon EC2 实例将持续录制并提供额外服务， CIs 因为录制范围为 “付费” 的服务关联录制器具有更高的录制频率

- 您需要为持续录制 Amazon EC2 实例付费
- 仅由您的客户管理的记录器记录的其他资源类型将继续按每日记录频率记录

受支持的服务

以下服务支持服务相关配置记录器：

Amazon service	服务主体	与一起使用的好处Amazon Config	了解详情
Amazon CloudWatch	`observabilityadmin.amazonaws.com`, `telemetry-enablement.observabilityadmin.amazonaws.com`	您可以使用 Amazon O CloudWatch bservability Admin 来发现和了解您的Amazon组织或账户 CloudWatch 的遥测配置状态。	有关更多信息，请参阅《CloudWatch 用户指南》中的审计 CloudWatch 遥测配置。
Amazon Security Hub CSPM	`securityhub.amazonaws.com`	您可以使用Amazon Security Hub CSPM 集中管理安全调查结果，并对Amazon账户进行安全评估。服务相关记录器支持以事件驱动的方法来获取暴露分析覆盖范围所需的资源配置项。	有关更多信息，请参阅 Sec urity Hub CSPM 用户指南中的启用 Security Hub。

配置记录器的偏离检测

`AWS::Config::ConfigurationRecorder` 资源类型是配置记录器的配置项（CI），用于跟踪配置记录器的所有状态更改。您可以使用此 CI 来检查配置记录器的状态是否与其先前的状态不同或已经偏离。

例如，该 CI 会跟踪是否对允许Amazon Config跟踪的资源类型进行了更新，是否停止或启动了配置记录器，或者是否删除或卸载了配置记录器。发生偏离的配置记录器表示您没有准确检测到预期资源类型的更改。如果您的配置记录器发生偏离，则可能导致漏报或误报合规性结果。

`AWS::Config::ConfigurationRecorder`资源类型是系统资源类型，默认情况下Amazon Config，所有支持的区域都启用了该资源类型的记录。`AWS::Config::ConfigurationRecorder`资源类型的记录不收取额外费用。

启动客户管理的配置记录器

您可以使用 Amazon Config 控制台或 Amazon CLI 启动客户管理的配置记录器。

To start the customer managed configuration recorder (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在导航窗格中，选择设置。
3. 在客户管理的记录器选项卡上，选择开始记录。出现提示时，选择确认。

To start the customer managed configuration recorder (CLI)

使用 `start-configuration-recorder` 命令：

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

停止客户管理的配置记录器

> **Note**
>
> 服务相关配置记录器始终处于记录状态
> 您无法停止服务相关配置记录器，因为服务相关配置记录器始终处于记录状态。要停止记录，必须删除服务相关配置记录器。有关更多信息，请参阅删除配置记录器。

您可以使用 Amazon Config 控制台或 Amazon CLI 来停止客户管理的配置记录器。

To stop the customer managed configuration recorder (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在导航窗格中，选择设置。
3. 在客户管理的记录器选项卡上，选择停止记录。出现提示时，选择确认。

To stop the customer managed configuration recorder (CLI)

使用 stop-configuration-recorder 命令：

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

更改客户管理的配置记录器的记录频率

Amazon Config 支持连续记录和每日记录。

- 连续记录可让您在每次发生配置更改时连续记录更改。
- 使用每日记录，您将收到代表过去 24 小时内资源的最新状态的配置项（CI），前提是它与之前记录的 CI 不同。有关更多信息，请参阅记录频率。

您可以使用 Amazon Config 控制台或 Amazon CLI 更改记录频率。

To change the recording frequency for the customer managed configuration recorder (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在导航窗格中，选择设置。
3. 在客户管理的记录器选项卡上，选择开始记录。
4. 对于 Recording method managed recorder，请选择 All resource types with customizable overrides。
5. 在默认设置中，选择记录频率。
6. 选择保存。

To change the recording frequency (CLI)

使用 put-configuration-recorder 命令更改配置记录器的记录频率：

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json
```

configurationRecorder.json 文件指定配置记录器的 name 和 roleArn 以及默认记录频率（recordingMode）。您也可以使用此字段来覆盖特定资源类型的记录频率。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include in
 the override ]
        }
    ]
  }
}
```

put-configuration-recorder 使用 --configuration-recorder 参数的以下字段：

- name：配置记录器的名称。Amazon Config 创建配置记录器时会自动分配“default”名称。
- roleARN：由 Amazon Config 代入并由配置记录器使用的 IAM 角色的 Amazon 资源名称（ARN）。
- recordingMode：指定 Amazon Config 用于记录配置更改的默认记录频率。Amazon Config 支持“连续记录”和“每日记录”。连续记录可让您在每次发生配置更改时连续记录更改。使用每日记录，您将收到代表过去 24 小时内资源的最新状态的配置项（CI），前提是它与之前记录的 CI 不同。
  - recordingFrequency：Amazon Config 用于记录配置更改的默认录制频率。

> **Note**
>
> Amazon Firewall Manager 依赖连续记录来监控您的资源。如果您使用的是 Firewall Manager，建议您将记录频率设置为“持续”。

- `recordingModeOverrides` – 此字段允许您为记录模式指定覆盖。它是一个 `recordingModeOverride` 对象数组。`recordingModeOverrides` 数组中的每个 `recordingModeOverride` 对象都由三个字段组成：
  - `description` – 您为覆盖提供的描述。
  - `recordingFrequency` – 将应用于覆盖中指定的所有资源类型的记录频率。
  - `resourceTypes` – 一个以逗号分隔的列表，用于指定 Amazon Config 在覆盖中包含哪些资源类型。

> **Note**
>
> 必填字段和可选字段
> [put-configuration-recorder](#) 的 `recordingMode` 字段是可选的。默认情况下，配置记录器的记录频率被设置为连续记录。

> **Note**
>
> 限制
> 以下资源类型不支持每日记录：
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`
>
> 对于记录所有当前和未来支持的资源类型（`ALL_SUPPORTED_RESOURCE_TYPES`）记录策略，这些资源类型将设置为“连续记录”。

重命名客户管理的配置记录器

必须使用 Amazon CLI 重命名客户管理的配置记录器。要更改客户管理的配置记录器的名称，您必须删除该配置记录器，然后使用指定名称创建一个新配置记录器。

使用 Amazon CLI 重命名客户管理的配置记录器

1. 使用 describe-configuration-recorders 命令查找当前客户管理的配置记录器的名称：

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

2. 使用 delete-configuration-recorder 命令删除客户管理的当前配置记录器：

```
$ 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客户管理的配置记录器：

```
$ 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
```

查看配置记录器

您可以使用 Amazon Config 控制台或 Amazon CLI 来查看有关配置记录器的详细信息。

To view your configuration recorders (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在导航窗格中，选择设置。
3. 对于客户管理的配置记录器，您可以在客户管理的记录器选项卡上查看详细信息。
4. 对于服务相关配置记录器，在服务相关记录器选项卡上选择服务相关配置记录器，然后选择查看。

To view your configuration recorders (CLI)

使用 describe-configuration-recorders 命令查看有关配置记录器的详细信息：

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

使用 describe-configuration-recorder-status 命令查找配置记录器的当前状态：

```
$ 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"
        }
    ]
}
```

对于这两个命令，您可以使用 `arn` 和 `configuration-recorder-names` 字段来指定配置记录器列表。对于服务相关配置记录器，您可以使用 `service-principal` 字段来指定配置记录器。

如果未指定配置记录器，则此命令将返回与该账户关联的所有配置记录器的详细信息。

删除配置记录器

必须使用 Amazon CLI 删除客户管理的配置记录器。您可以使用 Amazon Config 控制台或 Amazon CLI 删除服务相关配置记录器。

To delete the customer managed configuration recorder (CLI)

使用 `delete-configuration-recorder` 命令：

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

To delete a service-linked configuration recorder (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在导航窗格中，选择设置。
3. 在服务相关记录器选项卡上，选择一个服务相关配置记录器，然后选择删除。系统提示时，选择删除。

To delete a service-linked configuration recorder (CLI)

使用 `delete-service-linked-configuration-recorder` 命令：

此命令使用 `--service-principal` 字段。

```
$ aws configservice delete-service-linked-configuration-recorder --service-principal
 "The service principal of the Amazon Web Services ## for the service-linked
 configuration recorder that you want to delete"
```

使用传输通道

由于Amazon Config持续记录您的Amazon资源发生的变化，它会通过交付渠道发送通知和更新的配置状态。您可以管理交付渠道以控制配置更新的Amazon Config发送位置。

主题

- 注意事项
- 术语
- 配置项的组成部分
- 查看传输通道
- 更新传递通道
- 重命名传递通道
- 将配置快照传送到 Amazon S3 存储桶
- 验证传送状态
- 查看 Amazon S3 存储桶中的配置快照
- 示例配置快照来自Amazon Config
- Amazon Config 发送到 Amazon SNS 主题的通知

注意事项

每个账户的每个区域配有一个交付渠道

每个Amazon区域只能有一个配送渠道Amazon Web Services 账户，并且需要使用配送渠道Amazon Config。

超大配置项目通知包括简短摘要

当Amazon Config检测到资源的配置更改并且通知超过 Amazon SNS 允许的最大大小时，通知中会包含配置项目的简短摘要。您可以在 `s3BucketLocation` 字段中指定的 Amazon S3 存储桶位置查看完整通知。有关更多信息，请参阅过大配置项更改通知示例。

Amazon Config支持对使用的 Amazon S3 存储桶进行Amazon KMS加密Amazon Config

您可以提供Amazon Key Management Service(Amazon KMS) 密钥或别名亚马逊资源名称 (ARN) 来加密传输到您的亚马逊简单存储服务 (Amazon S3) 存储桶的数据。默认情况下，将配置历史记录和快照

文件Amazon Config传送到您的 Amazon S3 存储桶，并使用 S3 AES-256 服务器端加密 SSE-S3 对静态数据进行加密。但是，如果您提供Amazon Config了 KMS 密钥或别名 ARN，则Amazon Config使用该 KMS 密钥而不是 AES-256 加密。

Amazon Config不支持向 Amazon S3 存储桶的传送渠道，其中启用了对象锁定并启用了默认保留。有关更多信息，请参阅 S3 对象锁定的工作原理。

术语

配置项目表示您账户中存在的受支持Amazon资源的各种属性的 point-in-time视图。配置项目的组件包括元数据、属性、关系、当前配置和相关事件。Amazon Config每当它检测到正在记录的资源类型发生变化时，都会创建一个配置项目。例如，如果Amazon Config正在记录 Amazon S3 存储桶，则每当创建、更新或删除存储桶时，都会Amazon Config创建一个配置项目。您也可以选择Amazon Config以您设置的录制频率创建配置项目。

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。配置历史记录有多种格式可供您使用。Amazon Config自动将正在记录的每种资源类型的配置历史记录文件传送到您指定的 Amazon S3 存储桶。您可以在Amazon Config控制台中选择给定资源，然后使用时间轴导航到该资源的所有先前配置项目。此外，您还可以从 API 访问资源的历史配置项。

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，您还可以在Amazon Config控制台中选择一个时间点，并使用资源之间的关系浏览配置项目的快照。

配置流是自动更新的列表，列出了Amazon Config正在录制的资源的所有配置项目。每当资源被创建、修改或删除时，Amazon Config会创建一条配置项并将其添加到配置流。配置流使用您选择的 Amazon Simple Notification Service（Amazon SNS）主题工作。配置流有助于观察配置更改的发生，这样您就可以发现潜在的问题，在某些资源发生更改时生成通知，或者更新需要反映Amazon资源配置的外部系统。

配置项的组成部分

配置项 代表您账户中受支持的 Amazon 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，Amazon

Config 就会创建配置项。例如，如果 Amazon Config 正在记录 Amazon S3 存储桶，则只要创建、更新或删除存储桶，Amazon Config 就会创建配置项。您也可以选择让 Amazon Config 以您设置的记录频率创建配置项。

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	• 版本 ID • 捕获配置项的时间 • 表明项目是否成功捕获的配置项状态 • 表明资源配置项排序的状态 ID
属性	资源属性	• Resource ID • 此资源的键值标签列表 • 资源类型（请参阅支持的资源类型 Amazon Config） • 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
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` 附加到 Amazon EC2 实例 `i-a1b2c3d4`
当前配置	通过对资源进行 Describe 或 List API 调用返回的信息	例如，`DescribeVolumes` API 会返回有关卷的以下信息： • 卷所在的可用区 • 卷挂载的时间 • 卷挂载到的 EC2 实例的 ID • 卷的当前状态 • 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. 从 1.3 版开始，relatedEvents 字段为空。您可以访问《Amazon CloudTrail API 参考》中的 LookupEvents API，以检索资源事件。
3. 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。
4. 如果某资源类型不支持标签功能，或其描述性 API 响应中未包含标签信息，则 Amazon Config 不会在该资源类型的配置项（CI）中捕获标签数据。Amazon Config 仍会记录这些资源。但是，任何依赖标签数据的功能都将无法使用。这会影响依赖标签数据的基于标签的筛选、分组或合规性评估。

查看传输通道

您必须使用Amazon CLI来查看有关配送渠道的详细信息。

以下代码示例演示如何使用 `DescribeDeliveryChannels`。

CLI

Amazon CLI

获取有关传输通道的详细信息

以下命令返回有关传输通道的详细信息：

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

输出：

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI命令参考DescribeDeliveryChannels中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例检索该地区的传输通道并显示详细信息。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

输出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeDeliveryChannels中的。

适用于 PowerShell V5 的工具

示例 1：此示例检索该地区的传输通道并显示详细信息。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

输出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeDeliveryChannels中的。

更新传递通道

更新传递通道时，您可以设置以下选项：

- 用于Amazon Config发送配置快照和配置历史记录文件的 Amazon S3 存储桶。
- 将配置快照Amazon Config发送到您的 Amazon S3 存储桶的频率。
- 向其Amazon Config发送有关配置更改的通知的 Amazon SNS 主题。

更新传输通道（控制台）

您可以使用Amazon Config控制台为您的交付渠道设置 Amazon S3 存储桶和 Amazon SNS 主题。有关管理这些设置的步骤，请参阅 使用控制台设置 Amazon Config

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。要执行这些任务，必须使用Amazon CLI、Amazon Config API 或其中一个Amazon SDKs。

更新传递通道 (Amazon SDKs)

以下代码示例演示如何使用 `PutDeliveryChannel`。

CLI

Amazon CLI

创建传输通道

以下命令以 JSON 代码的形式提供传输通道的设置：

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

`deliveryChannel.json` 文件指定了传输通道的属性：

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

此示例设置了以下属性：

name——传输通道的名称。默认情况下，Amazon Config 会default将名称分配给新的交付渠道。您无法使用命令更新传递渠道名称。put-delivery-channel有关更改名称的步骤，请参阅“重命名传输通道”。s3BucketName-Amazon Config 向其发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另一个Amazon账户，则该存储桶必须具有授予对 Config Amazon的访问权限的策略。有关更多信息，请参阅 Amazon S3 存储桶的权限。

snsTopicARN-Amazon SNS 主题的亚马逊资源名称 (ARN)，Amazon Config 会向其发送有关配置变更的通知。如果您从其他账户选择主题，则该主题必须具有授予对 Config 的访问权限的策略。Amazon有关更多信息，请参阅 Amazon SNS 主题的权限。

configSnapshotDeliveryProperties-包含deliveryFrequency属性，该属性设置 Amazon Config 提供配置快照的频率以及它为定期 Config 规则调用评估的频率。

如果命令成功，Amazon Config 将不返回任何输出。要验证您的配送渠道的设置，请运行describe-delivery-channels命令。

- 有关 API 的详细信息，请参阅Amazon CLI命令参考PutDeliveryChannel中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例更改现有传输通道的 deliveryFrequency 属性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) PutDeliveryChannel中的。

适用于 PowerShell V5 的工具

示例 1：此示例更改现有传输通道的 deliveryFrequency 属性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) PutDeliveryChannel中的。

（可选）您可以使用 describe-delivery-channels 命令验证传输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"
        }
    ]
}
```

以下代码示例演示如何使用 DescribeDeliveryChannels。

CLI

Amazon CLI

获取有关传输通道的详细信息

以下命令返回有关传输通道的详细信息：

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

输出：

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI命令参考DescribeDeliveryChannels中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例检索该地区的传输通道并显示详细信息。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

输出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeDeliveryChannels中的。

适用于 PowerShell V5 的工具

示例 1：此示例检索该地区的传输通道并显示详细信息。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

输出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeDeliveryChannels中的。

重命名传递通道

要更改传递通道的名称，您必须删除该传输通道，然后使用指定名称创建一个新传输通道。在删除传递通道之前，您必须暂时停止配置记录器。Amazon Config控制台不提供删除传送渠道的选项。您必须使用Amazon CL Amazon Config I、API 或其中一个Amazon SDKs。

使用重命名配送渠道Amazon CLI

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

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

2. 使用 describe-delivery-channels 命令，并记下您的传输通道属性：

```
$ 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 命令删除传输通道：

```
$ 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输通道：

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

deliveryChannel.json 文件指定了传输通道的属性：

```
{
    "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
```

将配置快照传送到 Amazon S3 存储桶

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 Amazon Config 控制台中选择一个时间点，并按照资源之间的关系浏览不同配置项的快照。

传送配置快照

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

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

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

验证传送状态

输入`describe-delivery-channel-status`命令以验证是否Amazon Config已开始将配置传送到指定的交付渠道：

```
aws configservice describe-delivery-channel-status
```

该响应列出了Amazon Config用于向存储桶和主题传送配置的所有三种交付格式的状态。

```
{
```

```
    "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"
        }
    ]
}
```

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

> **Note**
>
> Amazon Config使用 UTC 格式（协调世界时）来记录时间。

查看 Amazon S3 存储桶中的配置快照

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，您还可以在Amazon Config控制台中选择一个时间点，并使用资源之间的关系浏览配置项目的快照。

查看配置快照

1. 登录Amazon Web Services 管理控制台并打开 Amazon S3 控制台，网址为https://console.aws.amazon.com/s3/。

2. 在 Amazon S3 控制台的所有存储桶列表中，选择 Amazon S3 存储桶名称。
3. 点阅查看您的存储桶中的嵌套文件夹，找到快照 ID 与由命令返回的 ID 相匹配的 `ConfigSnapshot` 对象。下载并打开对象以查看配置快照。S3 存储桶还包含一个名为的空文件`ConfigWritabilityCheckFile`。Amazon Config创建此文件以验证服务是否可以成功写入 S3 存储桶。

示例配置快照来自Amazon Config

以下是配置快照中Amazon Config包含的信息的示例。快照描述了在当前区域中为您录制的资源的配置 Amazon Web Services 账户，并描述了这些资源之间的关系。Amazon Config

> **Note**
>
> 配置快照可以包括对不支持的资源类型和资源的IDs 引用。


```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
```

```
                "name": "Attached to Instance"
            }
        ],
        "configuration": {
            "volumeId": "vol-ce676ccc",
            "size": 1,
            "snapshotId": "",
            "availabilityZone": "us-west-2b",
            "state": "in-use",
            "createTime": "2014-02-27T21:43:53.0885+0000",
            "attachments": [
                {
                    "volumeId": "vol-ce676ccc",
                    "instanceId": "i-344c463d",
                    "device": "/dev/sdf",
                    "state": "attached",
                    "attachTime": "2014-03-07T23:46:28.0000+0000",
                    "deleteOnTermination": false
                }
            ],
            "tags": [
                {
                    "tagName": "environment",
                    "tagValue": "PROD"
                },
                {
                    "tagName": "name",
                    "tagValue": "DataVolume1"
                }
            ],
            "volumeType": "standard"
        }
    },
    {
        "configurationItemVersion": "1.0",
        "resourceId": "i-344c463d",
        "accountId": "12345678910",
        "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
        "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
        "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
        "configurationItemStatus": "OK",
        "relatedEvents": [
            "06c12a39-eb35-11de-ae07-adb69edbb1e4",
            "c376e30d-71a2-4694-89b7-a5a04ad92281"
```

```
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
```

```
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
```

```
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
```

```
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

下一步是验证配置快照是否成功传送到了传递通道。

Amazon Config 发送到 Amazon SNS 主题的通知

> **Note**
>
> 必须先设置配置记录器和传输通道，然后 Amazon Config 才能向 Amazon SNS 主题发送通知。有关更多信息，请参阅管理配置记录器和管理传输通道。

可以配置，Amazon Config将配置更改和通知流式传输到 Amazon SNS 主题。例如，更新资源时，可以通过电子邮件接收通知，查看更改。也可以在 Amazon Config 针对您的资源评估自定义规则或托管规则时收到通知。有关更多信息，请参阅 Amazon Config 中的日志记录和监控。

Amazon Config 针对以下事件发送通知：

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

- Amazon Config 未能向您的账户传输通知。

主题

- 示例配置项变更通知
- 示例配置历史记录传输通知
- 示例配置快照传输开始通知
- 示例配置快照传输通知
- 示例合规性变更通知
- 示例规则评估开始通知
- 示例过大配置项变更通知
- 示例传输失败通知

示例配置项变更通知

Amazon Config使用 Amazon SNS 向订阅终端节点发送通知。这些通知提供配置快照和配置历史记录的交付状态，并提供记录Amazon资源的配置发生变化时Amazon Config创建的每个配置项目。Amazon Config还会发送通知，显示您的资源是否符合您的规则。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Amazon Config检测到 Amazon Elastic Block Store 卷 `vol-ce676ccc` 已附加到 ID 为 `i-344c463d` 的实例时，会生成该通知。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",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
```

```
            "awsAccountId": "123456789012",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [],
            "availabilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::VOLUME",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::INSTANCE",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [],
                "volumeType": "standard"
            }
        }
    ],
    "configurationItemDiff": {
        "changeType": "UPDATE",
        "changedProperties": {
            "Configuration.State": {
                "previousValue": "available",
                "updatedValue": "in-use",
                "changeType": "UPDATE"
```

```
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```


存在关系的资源的配置项

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

1. 您有一个 ID 为 Amazon EC2 实例`i-007d374c8912e3e90`，且该实例与亚马逊 EC2 安全组相关联`sg-c8b141b4`。
2. 您可以更新您的 EC2 实例，将安全组更改为另一个安全组`sg-3f1fef43`。
3. 由于该 EC2 实例与其他资源相关，因此Amazon Config会创建多个配置项目，如下例所示：

此通知包含替换安全组时 EC2 实例的配置项目更改。

```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
                        "macAddress": "0e:36:a2:2d:c5:e0",
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "sourceDestCheck": true,
                        "groups": [{
                            "groupName": "example-security-group-1",
                            "groupId": "sg-c8b141b4"
                        }],
                        "attachment": {
                            "attachmentId": "eni-attach-85bd89d9",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2017-01-09T19:36:02.000Z",
                            "deleteOnTermination": true
                        },
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
 "ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [{
                            "privateIpAddress": "172.31.16.84",
                            "privateDnsName": "ip-172-31-16-84.ec2.internal",
                            "primary": true,
                            "association": {
```

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

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

```
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
                    "name": "Is associated with SecurityGroup"
                },
                {
                    "resourceId": "subnet-2372be7b",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Subnet",
                    "name": "Is contained in Subnet"
                },
                {
                    "resourceId": "vol-0a2d63a256bce35c5",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Is attached to Volume"
                },
                {
                    "resourceId": "vpc-14400670",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::VPC",
                    "name": "Is contained in Vpc"
                }
            ],
            "configuration": {
                "instanceId": "i-007d374c8912e3e90",
                "imageId": "ami-9be6f38c",
                "state": {
                    "code": 16,
```

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

```
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
```

```
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


此通知包含与实例关联 EC2 的安全组的配置项目更改。sg-3f1fef43

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

```
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "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"
}
```


了解 Amazon SNS **ConfigurationItemChangeNotification** 通知中的 **configurationItemDiff** 字段

Amazon Config每当资源配置发生变化时，都会创建配置项目 (create/update/delete)。有关Amazon Config可以记录的支持资源类型的列表，请参阅支持的资源类型 Amazon Config。Amazon Config更改发生时使用 Amazon SNS 发送通知。Amazon SNS 通知有效负载包含可帮助您跟踪给定Amazon区域中的资源变化的字段。

要了解您收到 ConfigurationItemChangeNotification 通知的原因，请查看 configurationItemDiff 详细信息。这些字段因更改类型而异，可以形成不同的组合，例如 UPDATE-UPDATE、UPDATE-CREATE 和 DELETE-DELETE。以下是对一些常见组合的解释。

UPDATE-CREATE 和 UPDATE-UPDATE

以下示例包括资源直接关系和资源配置的更改。configurationItemDiff 详细信息显示以下信息：

已执行的操作：账户中存在的托管策略已关联到Amazon Identity and Access Management(IAM) 角色。

执行的基本操作：更新（更新账户中资源类型 AWS::IAM::Policy 的关联数量）。

更改类型组合：

1. 资源直接关系更改 UPDATE-CREATE。在 IAM 策略和 IAM 角色之间创建了新的附加或关联。
2. 资源配置更改 UPDATE-UPDATE。当策略附加到 IAM 角色时，IAM 策略关联的数量从 2 个增加到 3 个。

UPDATE-CREATE 和 UPDATE-UPDATE configurationItemDiff 通知示例：

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
                "updatedValue": {
                    "resourceId": "AROA6D3M4S53*********",
                    "resourceName": "Test1",
                    "resourceType": "AWS::IAM::Role",
                    "name": "Is attached to Role"
                },
                "changeType": "CREATE"                >>>>>>>>>>>>>>>>>>>> 1
            },
            "Configuration.AttachmentCount": {
                "previousValue": 2,
                "updatedValue": 3,
                "changeType": "UPDATE"                >>>>>>>>>>>>>>>>>>>> 2
            }
        },
        "changeType": "UPDATE"
    }
}
```

UPDATE-DELETE

以下示例包括资源直接关系和资源配置的更改。configurationItemDiff 详细信息显示以下信息：

已执行的操作：已从 IAM 用户分离账户中存在的托管策略。

已执行的基本操作：更新（更新与资源类型 AWS::IAM::User 关联的权限策略）。

更改类型组合：资源直接关系更改 UPDATE-DELETE。已删除账户中 IAM 用户与 IAM 策略之间的关联。

DELETE-DELETE

以下示例包括资源直接关系和资源配置的更改。configurationItemDiff 详细信息显示以下信息：

已执行的操作：已删除账户中存在的 IAM 角色。

已执行的基本操作：删除（已删除资源类型 AWS::IAM::Role 的资源）。

更改类型组合：资源直接关系更改和资源配置更改 DELETE-DELETE。删除 IAM 角色还会删除 IAM 策略与 IAM 角色的关联。

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。下面是在针对您的账户传输 CloudTrail 跟踪资源的配置历史记录时，Amazon Config 发送的通知示例。

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

```
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

示例配置快照传输开始通知

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

```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

示例配置快照传输通知

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

```
{
```

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

示例合规性变更通知

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

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

```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
```

```
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
```

```
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

示例：Config 配置项变更 | Amazon EventBridge

```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
```

```
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
```

```
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

示例规则评估开始通知

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

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

示例过大配置项变更通知

当 Amazon Config 检测到资源的配置变更时，会发送配置项（CI）通知。如果通知超过了 Amazon Simple Notification Service（Amazon SNS）允许的最大大小，则通知会包含配置项的简短摘要。

您可以在 s3BucketLocation 字段中指定的 Amazon S3 存储桶位置查看完整通知。

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

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

    New State Record Summary:
    ---------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:16.261Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "amzn-s3-demo-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"
    }
```

如何访问超大配置项

当配置项过大时，只会向 Amazon SNS 发送摘要。完整的配置项（CI）存储在 Amazon S3 中

以下代码示例显示如何访问您的完整 CI。

```
import boto3
import json

def handle_oversized_configuration_item(event):
    """
    Example of handling an oversized configuration item notification

    When a configuration item is oversized:
    1. AWS Config sends a summary notification through SNS
    2. The complete configuration item is stored in S3
    3. Use get_resource_config_history API to retrieve the complete configuration
    """

    # Extract information from the summary notification
    if event['messageType'] == 'OversizedConfigurationItemChangeNotification':
        summary = event['configurationItemSummary']
        resource_type = summary['resourceType']
        resource_id = summary['resourceId']

        # Initialize AWS Config client
        config_client = boto3.client('config')

        # Retrieve the complete configuration item
        response = config_client.get_resource_config_history(
            resourceType=resource_type,
            resourceId=resource_id
```

```
        )

        if response['configurationItems']:
            config_item = response['configurationItems'][0]

            # For EC2 instances, the configuration contains instance details
            configuration = json.loads(config_item['configuration'])
            print(f"Instance Configuration: {configuration}")

            # Handle supplementary configuration if present
            if 'supplementaryConfiguration' in config_item:
                for key, value in config_item['supplementaryConfiguration'].items():
                    if isinstance(value, str):
                        config_item['supplementaryConfiguration'][key] =
json.loads(value)
                print(f"Supplementary Configuration:
{config_item['supplementaryConfiguration']}")

            return config_item

        # If needed, you can also access the complete notification from S3
        s3_location = event['s3DeliverySummary']['s3BucketLocation']
        print(f"Complete notification available in S3: {s3_location}")

    return None
```

工作方式

1. 该函数接受包含 Amazon Config 通知的事件参数。
2. 它会检查消息类型是否为超大配置通知。
3. 该函数从摘要中提取资源类型和 ID。
4. 它使用 Amazon Config 客户端，检索完整的配置历史记录。
5. 该函数同时处理主配置和补充配置。
6. 如果需要，您可以从提供的 S3 位置访问完整通知。

示例传输失败通知

如果 Amazon Config 无法向 Amazon S3 存储桶传输配置快照或过大配置项更改通知，Amazon 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 the Console:
    https://console.aws.amazon.com/config/home?region=us-west-2#/timeline/
AWS::EC2::Instance/test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457?
time=2016-10-06T16:46:13.749Z

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

    New State Record Summary:
    --------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

查看 Amazon Config 控制面板

使用控制面板查看您的资源、规则、合规包及其合规状态的概述，并使用 Amazon CloudWatch 可视化您的 Amazon Config 使用情况和成功指标。此页面可帮助您快速识别 Amazon 账户中的热门资源，Amazon Web Services 账户中合规性级别最低的合规包，Amazon Web Services 账户中哪些规则或资源不合规，哪些流量推动了您的 Amazon Config 使用量，以及工作流程中出现的衡量成功和失败的关键指标。

使用 Amazon Config 控制面板

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

目录

- 合规性和资源清单
- Amazon Config 使用情况和成功指标

合规性和资源清单

安装后，Amazon Config 会开始记录指定的资源，并根据您的规则对其进行评估。Amazon Config 可能需要几分钟时间显示您的资源、规则、合规包及其合规性状态。

按合规性分数列出的合规包

按合规性分数列出的合规包最多显示 10 个合规性分数最低的合规包。合规性分数是合规包中的合规规则资源组合数量与合规包中可能的规则资源组合总数的百分比。

该指标为您提供合规包的合规性状态的简要视图，可用于识别、调查和了解合规包的合规性级别。您可以使用合规性分数来跟踪修正进度，对不同的需求集进行比较，并查看特定更改或部署对合规包的影响。

要在详细视图中查看合规包的部署状态、合规性分数、合规性分数时间线和规则，请选择合规包下的合规包的名称。

合规性状态

合规性状态显示您的合规和不合规规则以及合规和不合规资源的数量。根据对相关规则的评估，确定资源是合规还是不合规。如果资源不符合规则的规范，则该资源和规则将被标记为不合规。

要查看不合规规则和资源的列表，请选择不合规规则或不合规资源。

按不合规资源列出的规则

按不合规资源列出的规则按资源数量的降序显示排名靠前的不合规规则。选择一条规则以查看其详细信息、参数，以及该特定规则范围内的资源。

要查看不合规规则的完整列表，请选择查看所有不合规规则。

资源清单

资源清单按资源数量的降序显示 Amazon Config 记录的资源总数，以及您的 Amazon Web Services 账户中每种资源类型的计数。要打开某一资源类型的所有资源，请选择该资源类型以进入其资源清单页面。

您可以使用下拉列表来指明要查看哪些资源总计。默认情况下，它设置为查看所有资源，但您可以将其更改为 Amazon 资源、第三方资源或自定义资源。

> **Note**
>
> 使用 Config 规则评估您的 Amazon 资源配置消息可能会出于以下原因显示在控制面板上：
>
> - 您尚未为您的 Amazon Web Services 账户设置 Amazon Config 规则。您可以选择 Add rule 以转到 Rules 页面。
> - Amazon Config 仍在按照您的规则评估您的资源。您可以刷新该页面来查看最新的评估结果。
> - Amazon Config 根据您的规则评估您的资源，但没有在范围内找到任何资源。您可以在 Amazon ConfigSettings 页面中指定 要记录的资源。有关更多信息，请参阅 使用 Amazon Config 记录 Amazon 资源

Amazon Config 使用情况和成功指标

您可以在 Amazon Config 控制台中使用 Amazon CloudWatch 控制面板来直观显示您的 Amazon Config 使用情况和成功指标。

对于每个控制面板，您都可以执行以下操作：

- 调整控制面板的时间范围以显示过去 3 小时、1 天或 1 周的数据。
- 选择日历图标，输入自定义时间范围：过去指定时间的相对时间或两个日期之间的绝对时间范围。
- 您可以更改时间格式，以 UTC（协调世界时间）或本地时区（在设备操作系统中指定为本地时区的时区）显示控制面板数据。
- 使用刷新图标旁边的下拉箭头来指定控制面板中数据的刷新频率，或者关闭自动刷新。选择关闭、10 秒、1 分钟、2 分钟、5 分钟或 15 分钟来更改刷新间隔。
- 选择更多选项（垂直省略号菜单），将您当前在 Amazon Config 控制面板中查看的 Amazon Config 使用情况指标或 Amazon Config 成功指标添加到 CloudWatch 控制台。这会在 CloudWatch 控制台中打开一个新选项卡，允许您在 CloudWatch 中创建新的自定义控制面板，其中包含从当前 Amazon Config 使用情况指标或 Amazon Config 成功指标中复制的信息。

如果您想使用 CloudWatch 对这些指标进行其他分析，请在 CloudWatch 控制台的左侧导航窗格中选择指标，然后选择 Amazon/Config。有关您可以通过 CloudWatch 控制台执行的操作的更多信息，请参阅《CloudWatch 用户指南》中的使用 Amazon CloudWatch 控制面板和使用 Amazon CloudWatch 指标。

Amazon Config 使用情况指标

指标	描述	单位	
`ConfigurationItemsRecorded`	为每种资源类型或所有资源类型记录的配置项目数。配置项表示支持的 Amazon 资源的各种属性的时间点视图。有关配置项或支持的资源类型的更多信息，请参阅配置项和支持的资源类型。	计数	

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

Amazon Config 成功指标

指标	描述	单位	
`ChangeNotificat`	您的传输通道向 Amazon SNS 主题发送变更通知失败的次数。变更通知会通知您有关	计数	

指标	描述	单位	
ions Delivery Failed	Amazon 资源配置状态的变更情况。您可以使用 ConfigStreamDeliveryInfo API 获取上次尝试传输变更通知的 lastErrorCode 或。lastErrorMessage 有关更多信息，请参阅管理传输通道。		
Config History Export Failed	导出到您的 Amazon S3 存储桶的配置历史记录失败的数量。配置历史记录是给定资源在指定时间段的配置项集合。有关配置历史记录的更多信息，请参阅配置历史记录。	计数	
Configuration Recorder Insufficient Permissions Failure	由于您账户和 Amazon Web Services 区域中的所有配置记录器的 IAM 角色策略权限不足而导致的权限访问尝试失败的次数。配置记录器可检测范围内资源类型的更改。配置记录器需要具备必要的 IAM 权限，才能记录您的 Amazon 资源配置。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。	计数	
Config Snapshot Export Failed	导出到您的 Amazon S3 存储桶的配置快照失败的数量。配置快照是您账户中受支持资源的配置项集合。有关配置快照的更多信息，请参阅配置 | 快照。	计数	

管理和查看 Amazon Config 的 Amazon 资源配置

Amazon Config 可用于评测、审核和评估您的 Amazon 资源的配置。

Amazon 资源 是您使用、Amazon Web Services 管理控制台Amazon Command Line Interface（CLI）、Amazon 开发工具包或 Amazon 合作伙伴工具创建和管理的实体。Amazon 资源的示例包括 Amazon EC2 实例、安全组、Amazon VPC 和 Amazon Elastic Block Store。Amazon Config 使用其唯一标识符（例如，资源 ID 或 Amazon 资源名称（ARN））来参考每个资源。

一些常见使用案例包括：

- 云管理员：您可以跟踪和管理资源配置，以帮助确保合规性、排查问题并保持对 Amazon 环境的了解
- 安全分析师：您可以根据所需状态评估资源配置，以帮助识别漏洞和评估安全状况。
- 合规官员：您可以持续审核和监控资源配置，以帮助确保遵守组织政策和行业标准。

主题

- 支持的资源类型 Amazon Config
- 按区域可用性列出的资源覆盖范围
- 使用 Amazon Config 记录 Amazon 资源
- 使用 Amazon CLI 记录 Amazon Config 第三方资源的配置
- 使用 Amazon Config 记录托管实例的软件配置
- 查找 Amazon Config 发现的资源
- 使用查看Amazon资源的合规信息和评估结果Amazon Config
- 使用 Amazon Config 查看 Amazon 资源的合规性历史记录
- 查询 Amazon 资源的合规性历史记录
- 标记您的 Amazon Config 资源

支持的资源类型 Amazon Config

> **Important**
>
> 本页面会在每月初更新一次。

Amazon Config 支持以下 Amazon 资源类型和资源关系。

- 有关资源类型的更多详细信息，请参阅《 Amazon CloudFormation 用户指南》中Amazon 资源和属性类型参考中的参考信息（例如语法、属性和返回值）。
- 为了进行 Amazon Config 录制，某些 Amazon 地区支持这些资源类型的子集。有关哪些区域支持哪些资源类型的信息，请参阅按区域可用性列出的资源覆盖范围。
- 的高级查询 Amazon Config 支持这些资源类型的子集。有关那些支持的资源类型列表，请参阅支持的高级查询资源类型。
- 的主动评估 Amazon Config 支持这些资源类型中的一部分。有关那些支持的资源类型列表，请参阅主动评估支持的资源类型。
- 定期规则在不启用配置记录器的情况下运行，因为定期规则不依赖于配置项目（CIs）。有关变更触发规则和定期规则之间区别的更多信息，请参阅规则的评估模式和触发器 Amazon Config 类型。

  这意味着，如果您查看规则页面，其中不会列出 CI 或支持的资源。如果您选择资源 ID，将会看到以下错误：`The provided resource ID and resource type cannot be found`。这是预料之中的行为。

> **Note**
>
> 资源类型的区域可用性
> 在指定 Amazon Config 要跟踪的资源类型之前，请检查按区域可用性划分的资源覆盖率，以查看您设置的 Amazon 区域是否支持该资源类型 Amazon Config。如果至少有一个区域支持某种资源类型，则即使您设置的区域不支持指定的资源类型 Amazon Config，您也可以在支持的所有 Amazon 区域中启用该资源类型的记录 Amazon Config。 Amazon Config
> 资源类型的标签支持
> 如果资源类型不支持标记或在其 describe API 响应中不包含标签信息，则 Amazon Config 不会在该资源类型的配置项目 (CIs) 中捕获标签数据。 Amazon Config 仍将记录这些资源。但是，任何依赖标签数据的功能都将无法使用。这会影响依赖标签数据的基于标签的筛选、分组或合规性评估。

Amazon AppStream

Amazon 服务	资源类型值	关系	相关资源
Amazon AppStream	AWS::AppStream::Application	NA	NA
	AWS::AppStream::AppBlockBuilder	NA	NA
	AWS::AppStream::DirectoryConfig	NA	NA
	AWS::AppStream::Fleet	NA	NA
	AWS::AppStream::Stack	NA	NA

Amazon AppFlow

Amazon 服务	资源类型值	关系	相关资源
Amazon AppFlow	AWS::AppFlow::Flow	NA	NA

Amazon AppIntegrations

Amazon 服务	资源类型值	关系	相关资源
Amazon AppIntegrations	AWS::AppIntegratio	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	ns::Event Integration		
	AWS::AppI ntegratio ns::Appli cation	NA	NA

Amazon API Gateway

Amazon 服务	资源类型值	关系	相关资源
API Gateway	AWS::ApiG ateway::D omainName	NA	NA
	AWS::ApiG ateway::Stage	包含在	ApiGateway 休息 Api
		关联到	WAFRegional WebACL
	AWS::ApiG ateway::Method	NA	北美舞台
	AWS::ApiG ateway::R estApi	contains	ApiGateway 舞台
	AWS::ApiG ateway::U sagePlan	NA	NA
API Gateway V2	AWS::ApiG atewayV2: :Stage	包含在	ApiGatewayV2 Api

Amazon 服务	资源类型值	关系	相关资源
	AWS::ApiGatewayV2::Api	contains	ApiGatewayV2 舞台
	AWS::ApiGatewayV2::Integration	NA	NA

要详细了解如何 Amazon Config 与 Amazon API Gateway 集成，请参阅使用监控 API 网关 API 配置 Amazon Config。

Amazon Athena

Amazon 服务	资源类型值	关系	相关资源
Amazon Athena	AWS::Athena::WorkGroup	NA	NA
	AWS::Athena::DataCatalog	NA	NA
	AWS::Athena::PreparedStatement	NA	NA

Amazon Bedrock

Amazon 服务	资源类型值	关系	相关资源
Amazon Bedrock	AWS::Bedrock::ApplicationInferenceProfile	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::Bedrock::Guardrail	NA	NA
	AWS::Bedrock::KnowledgeBase	NA	NA
	AWS::Bedrock::Prompt	NA	NA
	AWS::BedrockAgentCore::BrowserCustom	NA	NA
	AWS::BedrockAgentCore::CodeInterpreterCustom	NA	NA
	AWS::BedrockAgentCore::Runtime	NA	NA

Amazon CloudFront

Amazon 服务	资源类型值	关系	相关资源
Amazon CloudFront	AWS::CloudFront::Distribution	关联到	Amazon WAF WebACL
			ACM 证书
			S3Bucket

Amazon 服务	资源类型值	关系	相关资源
			IAM 服务器证书
	AWS::CloudFront::KeyValueStore	NA	NA
	AWS::CloudFront::PublicKey	NA	NA
	AWS::CloudFront::StreamingDistribution	关联到	Amazon WAF WebACL
			ACM 证书
			S3Bucket
			IAM 服务器证书
	AWS::CloudFront::RealtimeLogConfig	NA	NA

Amazon CloudWatch

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

Amazon 服务	资源类型值	关系	相关资源
Amazon CloudWatch 日志	`AWS::Logs::Destination`	NA	NA
亚马逊 CloudWatch RUM	`AWS::RUM::AppMonitor`	NA	NA
CloudWatch 显然，亚马逊	`AWS::Evidently::Project`	NA	NA
	`AWS::Evidently::Launch`	NA	NA
	`AWS::Evidently::Segment`	NA	NA

Amazon CodeGuru

Amazon 服务	资源类型值	关系	相关资源
Amazon CodeGuru Reviewer	`AWS::CodeGuruReviewer::RepositoryAssociation`	NA	NA
Amazon P CodeGuru rofiler	`AWS::CodeGuruProfiler::ProfilingGroup`	NA	NA

Amazon Cognito

Amazon 服务	资源类型值	关系	相关资源
Amazon Cognito	AWS::Cognito::UserPool	NA	NA
	AWS::Cognito::UserPoolClient	NA	NA
	AWS::Cognito::UserPoolGroup	NA	NA
	AWS::Cognito::IdentityPool	NA	NA

Amazon Comprehend

Amazon 服务	资源类型值	关系	相关资源
Amazon Comprehend	AWS::Comprehend::Flywheel	NA	NA

Amazon Connect

Amazon 服务	资源类型值	关系	相关资源
Amazon Connect	AWS::Connect::PhoneNumber	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::Connect::QuickConnect	NA	NA
	AWS::Connect::Instance	NA	NA
	AWS::Connect::Rule	NA	NA
	AWS::Connect::SecurityProfile	NA	NA
	AWS::Connect::User	NA	NA
Amazon Connect Customer Profiles	AWS::CustomerProfiles::Domain	NA	NA
	AWS::CustomerProfiles::ObjectType	NA	NA

Amazon Detective

Amazon 服务	资源类型值	关系	相关资源
Amazon Detective	AWS::Detective::Graph	NA	NA

Amazon DynamoDB

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

Amazon Elastic Compute Cloud

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Compute Cloud	AWS::EC2::Host *	contains	EC2 实例
	AWS::EC2::EIP	挂载到	EC2 实例
			网络接口
	AWS::EC2::Instance	contains	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
			虚拟私有云（VPC）
	AWS::EC2::NetworkInterface	关联到	EC2 安全组
		挂载到	EC2 弹性 IP (EIP)
			EC2 实例

Amazon 服务	资源类型值	关系	相关资源
		包含在	路由表
			子网
			虚拟私有云（VPC）
	AWS::EC2::SecurityGroup *	关联到	EC2 实例
			EC2 网络接口
			虚拟私有云（VPC）
	AWS::EC2::NatGateway	包含在	虚拟私有云（VPC）
		包含在	子网
	AWS::EC2::EgressOnlyInternetGateway	挂载到	虚拟私有云（VPC）
	AWS::EC2::EC2Fleet	NA	NA
	AWS::EC2::SpotFleet	NA	NA
	AWS::EC2::SubnetNetworkAclAssociation	NA	NA
	AWS::EC2::PrefixList	NA	NA
	AWS::EC2::FlowLog	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::EC2::TransitGateway	NA	NA
	AWS::EC2::TransitGatewayAttachment	NA	NA
	AWS::EC2::TransitGatewayRouteTable	NA	NA
	AWS::EC2::VPCEndpoint	包含在	虚拟私有云（VPC）
		挂载到	网络接口
		包含在	子网
		包含在	路由表
	AWS::EC2::VPCEndpointService	关联到	ElasticLoadBalancingV2 LoadBalancer
	AWS::EC2::VPCPeeringConnection	关联到	虚拟私有云（VPC）
	AWS::EC2::RegisteredHAInstance	关联到	EC2 实例

Amazon 服务	资源类型值	关系	相关资源
	AWS::EC2::SubnetRouteTableAssociation	NA	NA
	AWS::EC2::LaunchTemplate	NA	NA
	AWS::EC2::NetworkInsightsAccessScopeAnalysis	NA	NA
	AWS::EC2::TrafficMirrorTarget	NA	NA
	AWS::EC2::TrafficMirrorSession	NA	NA
	AWS::EC2::DHCPOptions	NA	NA
	AWS::EC2::IPAM	NA	NA
	AWS::EC2::IPAMResourceDiscovery	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::EC2::IPAMResourceDiscoveryAssociation	NA	NA
	AWS::EC2::NetworkInsightsPath	NA	NA
	AWS::EC2::TrafficMirrorFilter	NA	NA
	AWS::EC2::CapacityReservation	NA	NA
	AWS::EC2::ClientVpnEndpoint	NA	NA
	AWS::EC2::CustomerGateway	挂载到	VPN 连接
	AWS::EC2::InternetGateway	挂载到	虚拟私有云（VPC）
	AWS::EC2::NetworkAcl	NA	NA
	AWS::EC2::RouteTable	contains	EC2 实例
			EC2 网络接口

Amazon 服务	资源类型值	关系	相关资源
			子网
			VPN 网关
		包含在	虚拟私有云（VPC）
	AWS::EC2::Subnet	contains	EC2 实例
			EC2 网络接口
		挂载到	网络 ACL
		包含在	路由表
			虚拟私有云（VPC）
	AWS::EC2::VPC	contains	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	互联网网关
			VPN 网关
	AWS::EC2::VPNConnection	挂载到	客户网关
			VPN 网关
	AWS::EC2::VPNConnectionRoute	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::EC2::VPNGateway	挂载到	虚拟私有云（VPC）
			VPN 连接
		包含在	路由表
	AWS::EC2::IPAMScope	NA	NA
	AWS::EC2::CarrierGateway	NA	NA
	AWS::EC2::TransitGatewayConnect	NA	NA
	AWS::EC2::IPAMPool	NA	NA
	AWS::EC2::TransitGatewayMulticastDomain	NA	NA
	AWS::EC2::NetworkInsightsAccessScope	NA	NA
	AWS::EC2::NetworkInsightsAnalysis	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::EC2::VPCBlockPublicAccessOptions	NA	NA
	AWS::EC2::VPCBlockPublicAccessExclusion	NA	NA
	AWS::EC2::EIPAssociation	NA	NA
	AWS::EC2::InstanceConnectEndpoint	NA	NA
	AWS::EC2::SnapshotBlockPublicAccess	NA	NA
	AWS::EC2::VPCEndpointConnectionNotification	NA	NA
	AWS::EC2::SecurityGroupVpcAssociation	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::EC2::VerifiedAccessInstance	NA	NA
	AWS::EC2::IPAMPoolCidr	NA	NA
	AWS::EC2::SubnetCidrBlock	NA	NA
	AWS::EC2::VPCGatewayAttachment	NA	NA
Amazon Elastic Block Store	AWS::EC2::Volume	挂载到	EC2 实例
EC2 Image Builder	AWS::ImageBuilder::ContainerRecipe	NA	NA
	AWS::ImageBuilder::DistributionConfiguration	NA	NA
	AWS::ImageBuilder::ImagePipeline	NA	NA
	AWS::ImageBuilder::ImageRecipe	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::ImageBuilder::InfrastructureConfiguration	NA	NA
	AWS::ImageBuilder::LifecyclePolicy	NA	NA

*Amazon Config 记录专用主机的配置详细信息以及您在这些主机上启动的实例。因此，当您报告服务器绑定软件许可证的合规性时，您可以 Amazon Config 将其用作数据源。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），以检查该主机是否符合 AMI 的许可证要求。有关更多信息，请参阅 Amazon EC2 用户指南 Amazon Config中的使用跟踪配置更改。

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

Amazon Elastic Container Registry

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

Amazon 服务	资源类型值	关系	相关资源
	ryCreatio nTemplate		
	AWS::ECR: :Registry Policy	NA	NA
	AWS::ECR: :PullThro ughCacheRule	NA	NA
Amazon Elastic Container Registry Public	AWS::ECR: :PublicRe pository	NA	NA

Amazon Elastic Container Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Container Service	AWS::ECS: :Cluster	NA	NA
	AWS::ECS: :TaskDefi nition	NA	NA
	AWS::ECS: :Service *	NA	NA
	AWS::ECS: :TaskSet	NA	NA
	AWS::ECS: :Capacity Provider	NA	NA

*此服务目前仅支持新的 Amazon 资源名称（ARN）格式。有关更多信息，请参阅 Amazon 资源名称 (ARNs) 和 IDs ECS 开发者指南。

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

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

Amazon Elastic File System

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

Amazon Elastic Kubernetes Service

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

Amazon EMR

Amazon 服务	资源类型值	关系	相关资源
Amazon EMR	AWS::EMR::Studio	NA	NA
	AWS::EMR::SecurityConfiguration	NA	NA
Amazon EMR 容器	AWS::EMRContainers::VirtualCluster	NA	NA

Amazon EMR Serverless

Amazon 服务	资源类型值	关系	相关资源
Amazon EMR Serverless	AWS::EMRServerless::Application	NA	NA

Amazon EventBridge

Amazon 服务	资源类型值	关系	相关资源
Amazon EventBridge	AWS::Events::EventBus	NA	NA
	AWS::Events::ApiDestination	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::Events::Archive	NA	NA
	AWS::Events::Endpoint	NA	NA
	AWS::Events::Connection	NA	NA
	AWS::Events::Rule	NA	NA
亚马逊 EventBridge 架构	AWS::EventSchemas::RegistryPolicy	NA	NA
	AWS::EventSchemas::Discoverer	NA	NA
	AWS::EventSchemas::Schema	NA	NA
	AWS::EventSchemas::Registry	NA	NA

Amazon Forecast

Amazon 服务	资源类型值	关系	相关资源
Amazon Forecast	AWS::Forecast::Dataset	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::Forecast::DatasetGroup	NA	NA

Amazon Fraud Detector

Amazon 服务	资源类型值	关系	相关资源
Amazon Fraud Detector	AWS::FraudDetector::Label	NA	NA
	AWS::FraudDetector::EntityType	NA	NA
	AWS::FraudDetector::Variable	NA	NA
	AWS::FraudDetector::Outcome	NA	NA

Amazon GameLift

Amazon 服务	资源类型值	关系	相关资源
Amazon GameLift	AWS::GameLift::Build	NA	NA

Amazon GuardDuty

Amazon 服务	资源类型值	关系	相关资源
Amazon GuardDuty	AWS::GuardDuty::Detector	NA	NA
	AWS::GuardDuty::Filter	NA	NA
	AWS::GuardDuty::IPSet	NA	NA
	AWS::GuardDuty::MalwareProtectionPlan	NA	NA
	AWS::GuardDuty::ThreatIntelSet	NA	NA

Amazon Inspector

Amazon 服务	资源类型值	关系	相关资源
Amazon Inspector	AWS::InspectorV2::Filter	NA	NA
	AWS::InspectorV2::Activation	NA	NA

Amazon Interactive Video Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Interactive Video Service	AWS::IVS::Channel	NA	NA
	AWS::IVS::RecordingConfiguration	NA	NA
	AWS::IVS::PlaybackKeyPair	NA	NA

Amazon Keyspaces（Apache Cassandra 兼容）

Amazon 服务	资源类型值	关系	相关资源
Amazon Keyspaces（Apache Cassandra 兼容）	AWS::Cassandra::Keyspace	NA	NA

Amazon Location Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Location Service	AWS::Location::APIKey	NA	NA

亚马逊 OpenSearch 服务

Amazon 服务	资源类型值	关系	相关资源
亚马逊 OpenSearch 服务（旧版 Elasticsearch）	`AWS::Elasticsearch::Domain`	关联到	KMS 密钥
			EC2 安全组
			EC2 子网
			虚拟私有云（VPC）
亚马逊 OpenSearch 服务	`AWS::OpenSearch::Domain`	NA	NA
Amazon OpenSearch 无服务器	`AWS::OpenSearchServerless::VpcEndpoint`	NA	NA
	`AWS::OpenSearchServerless::Collection`	NA	NA
	`AWS::OpenSearchServerless::SecurityConfig`	NA	NA

亚马逊 OpenSearch 服务重命名

2021 年 9 月 8 日，亚马逊 Elasticsearch 服务更名为亚马逊服务。 OpenSearch OpenSearch 服务支持 OpenSearch 以及传统的 Elasticsearch OSS。有关更多信息，请参阅 Amazon OpenSearch 服务-变更摘要。

即使您将一个或多个域名升级到，您也可能会在几周内继续在现有`AWS::Elasticsearch::Domain`资源类型`AWS::OpenSearch::Domain`下看到您的数据OpenSearch。

Amazon Personalize

Amazon 服务	资源类型值	关系	相关资源
Amazon Personalize	`AWS::Personalize::Dataset`	NA	NA
	`AWS::Personalize::Schema`	NA	NA
	`AWS::Personalize::Solution`	NA	NA
	`AWS::Personalize::DatasetGroup`	NA	NA

Amazon Pinpoint

Amazon 服务	资源类型值	关系	相关资源
Amazon Pinpoint	`AWS::Pinpoint::ApplicationSettings`	NA	NA
	`AWS::Pinpoint::Segment`	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::Pinpoint::App	NA	NA
	AWS::Pinpoint::Campaign	NA	NA
	AWS::Pinpoint::InAppTemplate	NA	NA
	AWS::Pinpoint::EmailChannel	NA	NA
	AWS::Pinpoint::EmailTemplate	NA	NA
	AWS::Pinpoint::EventStream	NA	NA

Amazon Quantum Ledger Database（Amazon QLDB）

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

Amazon Kendra

Amazon 服务	资源类型值	关系	相关资源
Amazon Kendra	`AWS::Kendra::Index`	NA	NA

Amazon Kinesis

Amazon 服务	资源类型值	关系	相关资源
Amazon Kinesis	`AWS::Kinesis::Stream`	NA	NA
	`AWS::Kinesis::StreamConsumer`	NA	NA
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	NA	NA
Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`	NA	NA
Kinesis 视频流	`AWS::KinesisVideo::SignalingChannel`	NA	NA
	`AWS::KinesisVideo::Stream`	NA	NA

Amazon Lex

Amazon 服务	资源类型值	关系	相关资源
Amazon Lex	AWS::Lex::BotAlias	NA	NA
	AWS::Lex::Bot	NA	NA

Amazon Lightsail

Amazon 服务	资源类型值	关系	相关资源
Amazon Lightsail	AWS::Lightsail::Disk	NA	NA
	AWS::Lightsail::Certificate	NA	NA
	AWS::Lightsail::Bucket	NA	NA
	AWS::Lightsail::StaticIp	NA	NA

Amazon Lookout for Metrics

Amazon 服务	资源类型值	关系	相关资源
Amazon Lookout for Metrics	AWS::LookoutMetrics::Alert	NA	NA

Amazon Lookout for Vision

Amazon 服务	资源类型值	关系	相关资源
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	NA	NA

Amazon Macie

Amazon 服务	资源类型值	关系	相关资源
Amazon Macie	`AWS::Macie::Session`	NA	NA

Amazon Managed Grafana

Amazon 服务	资源类型值	关系	相关资源
Amazon Managed Grafana	`AWS::Grafana::Workspace`	NA	NA

Amazon Managed Service for Prometheus

Amazon 服务	资源类型值	关系	相关资源
Amazon Managed Service for Prometheus	`AWS::APS::RuleGroupsNamespace`	NA	NA

Amazon MemoryDB

Amazon 服务	资源类型值	关系	相关资源
Amazon MemoryDB	`AWS::MemoryDB::SubnetGroup`	NA	NA

Amazon MQ

Amazon 服务	资源类型值	关系	相关资源
Amazon MQ	`AWS::AmazonMQ::Broker`	NA	NA

Amazon Managed Streaming for Apache Kafka

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

Amazon 服务	资源类型值	关系	相关资源
	AWS::MSK::VpcConnection	NA	NA
Amazon Managed Streaming for Apache Kafka Connect	AWS::KafkaConnect::Connector	NA	NA
	AWS::KafkaConnect::CustomPlugin	NA	NA

Amazon Quick Suite

Amazon 服务	资源类型值	关系	相关资源
Amazon Quick Suite	AWS::QuickSight::DataSource	NA	NA
	AWS::QuickSight::Template	NA	NA
	AWS::QuickSight::Theme	NA	NA

Amazon Redshift

Amazon 服务	资源类型值	关系	相关资源
Amazon Redshift	AWS::Redshift::Cluster	关联到	集群参数组
			集群安全组

Amazon 服务	资源类型值	关系	相关资源
			集群子网组
			安全组
			虚拟私有云（VPC）
	AWS::Redshift::ClusterParameterGroup	NA	NA
	AWS::Redshift::ClusterSecurityGroup	NA	NA
	AWS::Redshift::ScheduledAction	NA	NA
	AWS::Redshift::ClusterSnapshot	关联到	Cluster
			虚拟私有云（VPC）
	AWS::Redshift::ClusterSubnetGroup	关联到	子网
			虚拟私有云（VPC）
	AWS::Redshift::EventSubscription	NA	NA
	AWS::Redshift::EndpointAccess	NA	NA

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

Amazon Relational Database Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Relational Database Service	AWS::RDS::DBCluster	contains	RDS 数据库实例
		关联到	RDS 数据库子网组
			EC2 安全组
	AWS::RDS::DBClusterSnapshot	关联到	RDS 数据库集群
			虚拟私有云（VPC）
	AWS::RDS::DBInstance	关联到	EC2 安全组
			RDS 数据库安全组
			RDS 数据库子网组
	AWS::RDS::DBSecurityGroup	关联到	EC2 安全组
			虚拟私有云（VPC）
	AWS::RDS::DBSnapshot	关联到	虚拟私有云（VPC）

Amazon 服务	资源类型值	关系	相关资源
	AWS::RDS::DBSubnetGroup	关联到	EC2 安全组
			虚拟私有云（VPC）
	AWS::RDS::EventSubscription	NA	NA
	AWS::RDS::GlobalCluster	NA	NA
	AWS::RDS::Integration	NA	NA
	AWS::RDS::OptionGroup	NA	NA

Amazon Route 53

Amazon 服务	资源类型值	关系	相关资源
Amazon Route 53	AWS::Route53::DNSSEC	NA	NA
	AWS::Route53::HostedZone	NA	NA
	AWS::Route53::HealthCheck	NA	NA
Amazon Route 53 Profiles	AWS::Route53Profiles::Profile	NA	NA
	AWS::Route53Profiles::ProfileAssociation	NA	NA
Amazon Route 53 Resolver	AWS::Route53Resolver::ResolverEndpoint	NA	NA
	AWS::Route53Resolver::ResolverRule	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::Route53Resolver::ResolverRuleAssociation	NA	NA
	AWS::Route53Resolver::FirewallDomainList	NA	NA
	AWS::Route53Resolver::FirewallRuleGroupAssociation	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfig	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	NA	NA
	AWS::Route53Resolver::FirewallRuleGroup	NA	NA
Amazon 应用程序恢复控制器（ARC）	AWS::Route53RecoveryReadiness::Cell	NA	NA
	AWS::Route53RecoveryReadiness::ReadinessCheck	NA	NA
	AWS::Route53RecoveryReadiness::RecoveryGroup	NA	NA
	AWS::Route53RecoveryControl::Cluster	NA	NA
	AWS::Route53RecoveryControl::ControlPanel	NA	NA
	AWS::Route53RecoveryControl::RoutingControl	NA	NA
	AWS::Route53RecoveryControl::SafetyRule	NA	NA
	AWS::Route53RecoveryReadiness::ResourceSet	NA	NA

亚马逊 SageMaker AI

Amazon 服务	资源类型值	关系	相关资源	
亚马逊 SageMaker AI	AWS::SageMaker::AppImageConfig	NA	NA	
	AWS::SageMaker::CodeRepository	NA	NA	
	AWS::SageMaker::DataQualityJobDefinition	NA	NA	
	AWS::SageMaker::Domain	NA	NA	
	AWS::SageMaker::EndpointConfig	NA	NA	
	AWS::SageMaker::FeatureGroup	NA	NA	
	AWS::SageMaker::Image	NA	NA	

Amazon 服务	资源类型值	关系	相关资源	
	AWS::SageMaker::InferenceExperiment	NA	NA	
	AWS::SageMaker::MlflowTrackingServer	NA	NA	
	AWS::SageMaker::Model	NA	NA	
	AWS::SageMaker::ModelBiasJobDefinition	NA	NA	
	AWS::SageMaker::ModelExplainabilityJobDefinition	NA	NA	
	AWS::SageMaker::ModelQualityJobDefinition	NA	NA	

Amazon 服务	资源类型值	关系	相关资源	
	AWS::SageMaker::MonitoringSchedule	NA	NA	
	AWS::SageMaker::NotebookInstance	NA	NA	
	AWS::SageMaker::NotebookInstanceLifecycleConfig	NA	NA	
	AWS::SageMaker::StudioLifecycleConfig	NA	NA	
	AWS::SageMaker::UserProfile	NA	NA	
AWS::SageMaker::Workteam	NA	NA		

Amazon Simple Email Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Simple Email Service	AWS::SES::ConfigurationSet	NA	NA
	AWS::SES::ContactList	NA	NA
	AWS::SES::DedicatedIpPool	NA	NA
	AWS::SES::MailManagerTrafficPolicy	NA	NA
	AWS::SES::Template	NA	NA
	AWS::SES::ReceiptFilter	NA	NA
	AWS::SES::ReceiptRuleSet	NA	NA

Amazon Simple Notification Service

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

Amazon Simple Queue Service

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

Amazon Simple Storage Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Simple Storage Service	AWS::S3::Bucket *	NA	NA
	AWS::S3::AccountPublicAccessBlock	NA	NA
	AWS::S3::MultiRegionAccessPoint	NA	NA
	AWS::S3::StorageLens	NA	NA
	AWS::S3::AccessGrant	NA	NA
	AWS::S3::AccessGrantsInstance	NA	NA
	AWS::S3::AccessGrantsLocation	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::S3::AccessPoint	NA	NA
	AWS::S3::StorageLensGroup	NA	NA
	AWS::S3Tables::TableBucket	NA	NA
	AWS::S3Tables::TableBucketPolicy	NA	NA
Amazon S3 Express One Zone 存储类	AWS::S3Express::DirectoryBucket	NA	NA
	AWS::S3Express::BucketPolicy	NA	NA

* 如果您配置 Amazon Config 为记录 S3 存储桶，但未收到配置更改通知，请检查您的 S3 存储桶策略是否具有所需的权限。有关更多信息，请参阅 管理 S3 存储桶记录的权限。

Amazon S3 存储桶属性

Amazon Config 还记录了 Amazon S3 存储桶资源类型的以下属性。

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。

属性	说明
BucketPolicy	用于定义存储桶权限的策略。
CrossOriginConfiguration	允许跨区域请求存储桶。
LifecycleConfiguration	用于定义您存储桶中的对象生命周期的规则。
LoggingConfiguration	用于跟踪存储桶访问请求的日志记录。
NotificationConfiguration	用于针对指定存储桶事件发送警报或触发工作流的事件通知。
ReplicationConfiguration	在不同 Amazon 区域中的存储桶之间自动以异步方式复制对象。
RequestPaymentConfiguration	启用申请方付款。
TaggingConfiguration	添加到存储桶用于分类的标签。您也可以使用标记或跟踪计费。
WebsiteConfiguration	对存储桶启用静态网站托管。
VersioningConfiguration	对存储桶中的对象启用版本控制。

有关这些属性的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的存储桶配置选项。

Amazon WorkSpaces

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

Amazon Amplify

Amazon 服务	资源类型值	关系	相关资源
Amazon Amplify	AWS::Amplify::App	NA	NA
	AWS::Amplify::Branch	NA	NA

Amazon AppConfig

Amazon 服务	资源类型值	关系	相关资源
Amazon AppConfig	AWS::AppConfig::Application	NA	NA
	AWS::AppConfig::Environment	NA	NA
	AWS::AppConfig::ConfigurationProfile	NA	NA
	AWS::AppConfig::DeploymentStrategy	NA	NA
	AWS::AppConfig::HostedConfi	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	gurationV ersion		
	AWS::AppC onfig::Ex tension	NA	NA
	AWS::AppC onfig::Ex tensionAs sociation	NA	NA

Amazon App Runner

Amazon 服务	资源类型值	关系	相关资源
Amazon App Runner	AWS::AppR unner::Vp cConnector	NA	NA
	AWS::AppR unner::Service	NA	NA

Amazon App Mesh

Amazon 服务	资源类型值	关系	相关资源
Amazon App Mesh	AWS::AppM esh::Virt ualNode	NA	NA
	AWS::AppM esh::Virt ualService	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::AppMesh::VirtualGateway	NA	NA
	AWS::AppMesh::VirtualRouter	NA	NA
	AWS::AppMesh::Route	NA	NA
	AWS::AppMesh::GatewayRoute	NA	NA
	AWS::AppMesh::Mesh	NA	NA

Amazon AppSync

Amazon 服务	资源类型值	关系	相关资源
Amazon AppSync	AWS::AppSync::GraphQLApi	NA	NA

Amazon Audit Manager

Amazon 服务	资源类型值	关系	相关资源
Amazon Audit Manager	AWS::AuditManager::Assessment	NA	NA

Amazon Auto Scaling

Amazon 服务	资源类型值	关系	相关资源
Amazon Auto Scaling	AWS::AutoScaling::AutoScalingGroup	contains	亚马逊 EC2 实例
		关联到	Classic 负载均衡器
			Auto Scaling 启动配置
			子网
	AWS::AutoScaling::LaunchConfiguration	关联到	亚马逊 EC2 安全组
	AWS::AutoScaling::ScalingPolicy	关联到	自动扩缩组
			警报
	AWS::AutoScaling::ScheduledAction	关联到	自动扩缩组
	AWS::AutoScaling::WarmPool	NA	NA

Amazon B2B 数据交换

Amazon 服务	资源类型值	关系	相关资源
Amazon B2B 数据交换	AWS::B2BI::Capability	NA	NA

Amazon Backup

Amazon 服务	资源类型值	关系	相关资源
Amazon Backup	AWS::Backup::BackupPlan	NA	不适用*
	AWS::Backup::BackupSelection	NA	NA
	AWS::Backup::BackupVault	NA	不适用*
	AWS::Backup::RecoveryPoint	NA	NA
	AWS::Backup::ReportPlan	NA	NA
	AWS::Backup::RestoreTestingPlan	Na	NA
Amazon Backup 网关	AWS::BackupGateway::Hypervisor	NA	NA

由于 Amazon Backup 工作原理，其中一些资源类型与下表中的其他 Amazon Backup 资源类型相关。

AWS::Backup::BackupPlan与 Backup Plan 有许多选择的AWS::Backup::RecoveryPoint位置有关，AWS::Backup::BackupVault也与 Amazon Backup Vault 有多个恢复点的位置有关。AWS::Backup::BackupSelection

有关更多信息，请参阅使用备份计划管理备份和使用备份保管库。

Amazon Batch

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

Amazon 账单与成本管理

Amazon 服务	资源类型值	关系	相关资源
Amazon 账单与成本管理	AWS::BCMDataExports::Export	NA	NA

Amazon Budgets

Amazon 服务	资源类型值	关系	相关资源
Amazon Budgets	AWS::Budgets::BudgetsAction	NA	NA

Amazon Certificate Manager

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

Amazon 干净的房间

Amazon 服务	资源类型值	关系	相关资源
Amazon 无尘室机器学习	`AWS::CleanRoomsML::TrainingDataset`	NA	NA

Amazon CloudFormation

Amazon 服务	资源类型值	关系	相关资源
Amazon CloudFormation	`AWS::CloudFormation::GuardHook`	NA	NA
	`AWS::CloudFormation::LambdaHook`	NA	NA
	`AWS::CloudFormation::Stack` *	contains	支持的 Amazon 资源类型
	`AWS::CloudFormation::StackSet`	NA	NA

*Amazon Config 记录堆栈的配置更改以及 Amazon CloudFormation 堆栈中支持的资源类型。 Amazon Config 不记录堆栈中尚不支持的资源类型的配置更改。不受支持的资源类型显示在堆栈的配置项的补充配置部分中。

Amazon CloudTrail

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

Amazon Cloud9

Amazon 服务	资源类型值	关系	相关资源
Amazon Cloud9	`AWS::Cloud9::EnvironmentEC2`	NA	NA

Amazon Cloud9 新用户不再可以访问权限

经过仔细考虑，我们决定从 2024 年 7 月 25 Amazon Cloud9日起关闭新客户的访问权限。Amazon Cloud9 现有客户可以继续照常使用该服务。 Amazon 继续投资于安全性、可用性和性能改进 Amazon Cloud9，但我们不打算引入新功能。有关更多信息，请参阅如何从 IDE 工具包迁移 Amazon Cloud9 到 Amazon IDE 工具包或 Amazon CloudShell。

Amazon Cloud Map

Amazon 服务	资源类型值	关系	相关资源
服务发现	AWS::ServiceDiscovery::Service	NA	NA
	AWS::ServiceDiscovery::PublicDnsNamespace	NA	NA
	AWS::ServiceDiscovery::HttpNamespace	NA	NA
AWS::ServiceDiscovery::Instance	NA	NA	

Amazon CodeArtifact

Amazon 服务	资源类型值	关系	相关资源
Amazon CodeArtifact	AWS::CodeArtifact::Repository	NA	NA
	AWS::CodeArtifact::Domain	NA	NA

Amazon CodeBuild

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

* 要详细了解如何与 Amazon Config 集成 Amazon CodeBuild，请参阅Amazon Config 与 Amazon CodeBuild 示例一起使用。

Amazon CodeDeploy

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

Amazon CodePipeline

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

*Amazon Config 记录 CodePipeline 管道的配置更改以及管道中支持的资源类型。 Amazon Config 不记录管道中尚不支持的资源类型的配置更改。不受支持的资源类型（如 `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, 和 `ECS service`）显示在堆栈的配置项的补充配置部分中。

Amazon Config

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

Amazon 服务	资源类型值	关系	相关资源
	rmancePac kCompliance		
	AWS::Conf ig::Confi gurationR ecorder *	NA	NA
	AWS::Conf ig::Confo rmancePack	NA	NA
	AWS::Conf ig::Store dQuery	NA	NA

* AWS::Config::ResourceCompliance 与相关资源之间的关系取决于 AWS::Config::ResourceCompliance 如何报告该特定资源类型的合规性。

* AWS::Config::ConfigurationRecorder 是系统资源类型，默认情况下 Amazon Config ，此资源类型的记录处于启用状态。

> **Note**
>
> 记录 AWS::Config::ConformancePackCompliance 和 AWS::Config::ConfigurationRecorder 资源类型不收取额外费用。

Amazon Database Migration Service

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

Amazon 服务	资源类型值	关系	相关资源
	AWS::DMS::ReplicationSubnetGroup	NA	NA
	AWS::DMS::ReplicationInstance	NA	NA
	AWS::DMS::ReplicationTask	NA	NA
	AWS::DMS::Certificate	NA	NA
	AWS::DMS::Endpoint	NA	NA

Amazon DataSync

Amazon 服务	资源类型值	关系	相关资源
Amazon DataSync	AWS::DataSync::Agent	NA	NA
	AWS::DataSync::LocationSMB	NA	NA
	AWS::DataSync::LocationFSxLustre	NA	NA
	AWS::DataSync::Loc	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	ationFSxWindows		
	AWS::DataSync::LocationS3	NA	NA
	AWS::DataSync::LocationEFS	NA	NA
	AWS::DataSync::LocationNFS	NA	NA
	AWS::DataSync::LocationHDFS	NA	NA
	AWS::DataSync::LocationObjectStorage	NA	NA
	AWS::DataSync::Task	NA	NA

Amazon 截止日期云

Amazon 服务	资源类型值	关系	相关资源
Amazon 截止日期云	AWS::Deadline::Fleet	NA	NA
	AWS::Deadline::Monitor	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::Deadline::QueueFleetAssociation	NA	NA

Amazon Device Farm

Amazon 服务	资源类型值	关系	相关资源
Amazon Device Farm	AWS::DeviceFarm::TestGridProject	NA	NA
	AWS::DeviceFarm::InstanceProfile	NA	NA
	AWS::DeviceFarm::Project	NA	NA

Amazon Elastic Beanstalk

Amazon 服务	资源类型值	关系	相关资源
Amazon Elastic Beanstalk	AWS::ElasticBeanstalk::Application	contains	Elastic Beanstalk 应用程序版本
			Elastic Beanstalk 环境
		关联到	IAM 角色
	AWS::ElasticBeanst	包含在	Elastic Beanstalk 应用程序

Amazon 服务	资源类型值	关系	相关资源
	alk::Appl icationVersion	关联到	Elastic Beanstalk 环境
			S3 存储桶
	AWS::Elas ticBeanst alk::Envi ronment	包含在	Elastic Beanstalk 应用程序
		关联到	Elastic Beanstalk 应用程序版本
			IAM 角色
		contains	CloudFormation 堆栈

Amazon Entity Resolution 数据匹配服务

Amazon 服务	资源类型值	关系	相关资源
Amazon Entity Resolution 数据匹配服务	AWS::Enti tyResolut ion::IdMa ppingWorkflow	NA	NA
	AWS::Enti tyResolut ion::Matc hingWorkflow	NA	NA
	AWS::Enti tyResolut ion::Sche maMapping	NA	NA

Amazon Fault Injection Service

Amazon 服务	资源类型值	关系	相关资源
Amazon Fault Injection Service	`AWS::FIS::ExperimentTemplate`	NA	NA

Amazon Global Accelerator

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

Amazon Glue

Amazon 服务	资源类型值	关系	相关资源
Amazon Glue	`AWS::Glue::Job`	NA	NA
	`AWS::Glue::Classifier`	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::Glue::MLTransform	NA	NA
	AWS::Glue::Database	NA	NA
	AWS::Glue::Registry	NA	NA

Amazon Ground Station

Amazon 服务	资源类型值	关系	相关资源
Amazon Ground Station	AWS::GroundStation::Config	NA	NA
	AWS::GroundStation::MissionProfile	NA	NA
	AWS::GroundStation::DataflowEndpointGroup	NA	NA

Amazon HealthLake

Amazon 服务	资源类型值	关系	相关资源
Amazon HealthLake	`AWS::HealthLake::FHIRDatastore`	NA	NA

Amazon Identity and Access Management (IAM)

Amazon 服务	资源类型值	关系	相关资源
Amazon Identity and Access Management	`AWS::IAM::User`	挂载到	IAM 组
			IAM 客户托管策略
	`AWS::IAM::Group`	contains	IAM 用户
		挂载到	IAM 客户托管策略
	`AWS::IAM::Role`	挂载到	IAM 客户托管策略
	`AWS::IAM::Policy`	挂载到	IAM 用户
			IAM 组
			IAM 角色
	`AWS::IAM::SAMLProvider`	NA	NA
	`AWS::IAM::ServerCertificate`	NA	NA
	`AWS::IAM::InstanceProfile`	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::IAM::OIDCProvider	NA	NA
Amazon Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	NA	NA
Amazon Identity and Access Management 角色随处可见	AWS::RolesAnywhere::Profile	NA	NA
	AWS::RolesAnywhere::CRL	NA	NA
	AWS::RolesAnywhere::TrustAnchor	NA	NA

Amazon Config 包括内联策略及其记录的配置详细信息。有关内联策略的更多信息，请参阅《IAM 用户指南》中的托管式策略与内联策略。

Amazon IoT

Amazon 服务	资源类型值	关系	相关资源
Amazon IoT	AWS::IoT::AccountAuditConfiguration	NA	NA
	AWS::IoT::Authorizer	NA	NA
	AWS::IoT::CACertificate	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::IoT::CustomMetric	NA	NA
	AWS::IoT::Dimension	NA	NA
	AWS::IoT::DomainConfiguration	NA	NA
	AWS::IoT::JobTemplate	NA	NA
	AWS::IoT::MitigationAction	NA	NA
	AWS::IoT::Policy	NA	NA
	AWS::IoT::ProvisioningTemplate	NA	NA
	AWS::IoT::RoleAlias	NA	NA
	AWS::IoT::ScheduledAudit	NA	NA
	AWS::IoT::SecurityProfile	NA	NA
	AWS::IoT::ThingGroup	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::IoTSiteWise::Gateway	NA	NA
Amazon IoT Wireless	AWS::IoTWireless::ServiceProfile	NA	NA
	AWS::IoTWireless::MulticastGroup	NA	NA
	AWS::IoTWireless::FuotaTask	NA	NA
Amazon IoT Core	AWS::IoT::FleetMetric	NA	NA
Amazon IoT Core 设备顾问	AWS::IoTCoreDeviceAdvisor::SuiteDefinition	NA	NA
Amazon IoT Analytics	AWS::IoTAnalytics::Datastore	NA	NA
	AWS::IoTAnalytics::Dataset	NA	NA
	AWS::IoTAnalytics::Pipeline	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::IoTAnalytics::Channel	NA	NA
Amazon IoT Events	AWS::IoTEvents::Input	NA	NA
	AWS::IoTEvents::DetectorModel	NA	NA
	AWS::IoTEvents::AlarmModel	NA	NA
Amazon IoT TwinMaker	AWS::IoTTwinMaker::Workspace	NA	NA
	AWS::IoTTwinMaker::Entity	NA	NA
	AWS::IoTTwinMaker::Scene	NA	NA
	AWS::IoTTwinMaker::SyncJob	NA	NA
	AWS::IoTTwinMaker::ComponentType	NA	NA
Amazon IoT SiteWise	AWS::IoTSiteWise::Asset	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::IoTSiteWise::AssetModel	NA	NA
	AWS::IoTSiteWise::Dashboard	NA	NA
	AWS::IoTSiteWise::Portal	NA	NA
	AWS::IoTSiteWise::Project	NA	NA
Amazon IoT Greengrass Version 2	AWS::GreengrassV2::ComponentVersion	NA	NA

Amazon Key Management Service

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

Amazon Lambda

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

Amazon Mainframe Modernization

Amazon 服务	资源类型值	关系	相关资源
Amazon Mainframe Modernization	AWS::M2::Environment	NA	NA

Amazon Network Firewall

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

Amazon 服务	资源类型值	关系	相关资源
	AWS::NetworkFirewall::RuleGroup	NA	NA
	AWS::NetworkFirewall::TLSInspectionConfiguration	NA	NA
	AWS::NetworkFirewall::VpcEndpointAssociation	NA	NA

Amazon Network Manager

Amazon 服务	资源类型值	关系	相关资源
Amazon Network Manager	AWS::NetworkManager::TransitGatewayRegistration	NA	NA
	AWS::NetworkManager::Site	NA	NA
	AWS::NetworkManager::Device	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::NetworkManager::Link	NA	NA
	AWS::NetworkManager::GlobalNetwork	NA	NA
	AWS::NetworkManager::CustomerGatewayAssociation	NA	NA
	AWS::NetworkManager::LinkAssociation	NA	NA
	AWS::NetworkManager::ConnectPeer	NA	NA
	AWS::NetworkManager::TransitGatewayPeering	NA	NA

Amazon 组织

Amazon 服务	资源类型值	关系	相关资源
Amazon 组织	`AWS::Organizations::OrganizationalUnit`	NA	NA

Amazon Panorama

Amazon 服务	资源类型值	关系	相关资源
Amazon Panorama	`AWS::Panorama::Package`	NA	NA

Amazon 私有证书颁发机构

Amazon 服务	资源类型值	关系	相关资源
Amazon 私有证书颁发机构	`AWS::ACMPCA::CertificateAuthority`	NA	NA
	`AWS::ACMPCA::CertificateAuthorityActivation`	NA	NA
Amazon 私有 CA 活动目录连接器	`AWS::PCAConnectorAD::Connector`	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	AWS::PCAConnectorAD::DirectoryRegistration	NA	NA

Amazon Resilience Hub

Amazon 服务	资源类型值	关系	相关资源
Amazon Resilience Hub	AWS::ResilienceHub::ResiliencyPolicy	NA	NA
	AWS::ResilienceHub::App	NA	NA

Amazon 资源探索器

Amazon 服务	资源类型值	关系	相关资源
Amazon 资源探索器	AWS::ResourceExplorer2::Index	NA	NA

Amazon RoboMaker

Amazon 服务	资源类型值	关系	相关资源
Amazon RoboMaker	AWS::RoboMaker::Ro	NA	NA

Amazon 服务	资源类型值	关系	相关资源
	botApplicationVersion		
	AWS::RoboMaker::RobotApplication	NA	NA
	AWS::RoboMaker::SimulationApplication	NA	NA

Amazon Signer

Amazon 服务	资源类型值	关系	相关资源
Amazon Signer	AWS::Signer::SigningProfile	NA	NA

Amazon Secrets Manager

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

Amazon 服务	资源类型值	关系	相关资源
	AWS::SecretsManager::RotationSchedule	NA	NA

Amazon Security Hub CSPM

Amazon 服务	资源类型值	关系	相关资源
Amazon Security Hub CSPM	AWS::SecurityHub::Standard	NA	NA

Amazon Service Catalog

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

> **Note**
>
> Amazon Service Catalog 与一起使用时 Amazon Config，配置项目会显示子配置产品的 ARN，而不是父产品的 ARN。当 Amazon Service Catalog 预配置产品充当父预配置产品中的资源时，就会发生这种情况。 CloudFormation资源 ID 仍可通过 Amazon Config 接口进行跟踪。

Amazon Shield

Amazon 服务	资源类型值	关系	相关资源
Amazon Shield	`AWS::Shield::Protection`	关联到	亚马逊 CloudFront 配送
	`AWS::ShieldRegional::Protection`	关联到	EC2 EIP
		关联到	ElasticLoadBalancing 平衡器
		关联到	ElasticLoadBalancingV2 LoadBalancer

Amazon Step Functions

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

Amazon Systems Manager

Amazon 服务	资源类型值	关系	相关资源
Amazon Systems Manager	AWS::SSM::ManagedInstanceInventory *	关联到	EC2 实例
	AWS::SSM::PatchCompliance	关联到	托管实例清单
	AWS::SSM::AssociationCompliance	关联到	托管实例清单
	AWS::SSM::FileData	关联到	托管实例清单
	AWS::SSM::Document	NA	NA
	AWS::SSM::ResourceDataSync	NA	NA
Amazon Systems Manager Incident Manager	AWS::SSMIncidents::ResponsePlan	NA	NA
Amazon Systems Manager Incident Manager 联系人	AWS::SSMContacts::Contact	NA	NA

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

Amazon Transfer Family

Amazon 服务	资源类型值	关系	相关资源
Amazon Transfer Family	AWS::Transfer::Agreement	NA	NA
	AWS::Transfer::Connector	NA	NA
	AWS::Transfer::Workflow	NA	NA
	AWS::Transfer::Certificate	NA	NA
	AWS::Transfer::Profile	NA	NA
	AWS::Transfer::Server	NA	NA

Amazon WAF

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

Amazon 服务	资源类型值	关系	相关资源
			WAF Rulegroup
	AWS::WAF::RuleGroup	关联到	WAF 规则
	AWS::WAFRegional::RateBasedRule	NA	NA
	AWS::WAFRegional::Rule	NA	NA
	AWS::WAFRegional::WebACL	关联到	ElasticLoadBalancingV2 LoadBalancer
			WAFRegional 规则
			WAFRegional 基于费率的规则
			WAFRegional 规则组
	AWS::WAFRegional::RuleGroup	关联到	WAFRegional 规则
Amazon WAF V2	AWS::WAFv2::WebACL	关联到	ElasticLoadBalancingV2 LoadBalancer
			ApiGateway 舞台
			WAFv2 IPSet
			WAFv2 RegexPatternSet
			WAFv2 RuleGroup

Amazon 服务	资源类型值	关系	相关资源
			WAFv2 ManagedRuleSet
	AWS::WAFv2::RuleGroup	关联到	WAFv2 IPSet
			WAFv2 RegexPatternSet
	AWS::WAFv2::ManagedRuleSet	关联到	WAFv2 RuleGroup
	AWS::WAFv2::IPSet	NA	NA
	AWS::WAFv2::RegexPatternSet	NA	NA

Amazon X-Ray

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

Elastic Load Balancing

Amazon 服务	资源类型值	关系	相关资源
Elastic Load Balancing	应用程序负载均衡器	关联到	EC2 安全组
		挂载到	子网

Amazon 服务	资源类型值	关系	相关资源
	AWS::ElasticLoadBalancingV2::LoadBalancer	包含在	虚拟私有云（VPC）
	应用程序负载均衡器侦听器 AWS::ElasticLoadBalancingV2::Listener	NA	NA
	Application Load Balancer 目标 AWS::ElasticLoadBalancingV2::TargetGroup	NA	NA
	Classic 负载均衡器 AWS::ElasticLoadBalancing::LoadBalancer	关联到	EC2 安全组
		挂载到	子网
		包含在	虚拟私有云（VPC）
	网络负载均衡器 AWS::ElasticLoadBalancingV2::LoadBalancer	NA	NA

AWS Elemental MediaConnect

Amazon 服务	资源类型值	关系	相关资源
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	NA	NA
	`AWS::MediaConnect::FlowVpcInterface`	NA	NA
	`AWS::MediaConnect::FlowSource`	NA	NA
	`AWS::MediaConnect::Gateway`	NA	NA

AWS Elemental MediaPackage

Amazon 服务	资源类型值	关系	相关资源
AWS Elemental MediaPackage	`AWS::MediaPackage::PackagingGroup`	NA	NA
	`AWS::MediaPackage::PackagingConfiguration`	NA	NA

AWS Elemental MediaPackage V2

Amazon 服务	资源类型值	关系	相关资源
AWS Elemental MediaPackage V2	`AWS::MediaPackageV2::Channel`	NA	NA
	`AWS::MediaPackageV2::ChannelGroup`	NA	NA
	`AWS::MediaPackageV2::OriginEndpoint`	NA	NA

AWS Elemental MediaTailor

Amazon 服务	资源类型值	关系	相关资源
AWS Elemental MediaTailor	`AWS::MediaTailor::LiveSource`	NA	NA
	`AWS::MediaTailor::PlaybackConfiguration`	NA	NA

按区域可用性列出的资源覆盖范围

北美洲和南美洲区域

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::ACM::Certificate	是	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority	是	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority激活	是	是	是	是	是	是	是	是
AWS::APS::RuleGroups命名空间	没有	是	是	是	没有	没有	是	是
AWS::AccessAnalyzer::Analyzer	是	是	是	是	是	是	是	是
AWS::AmazonMQ::Broker	是	是	是	是	没有	是	没有	是
AWS::Amplify::App	是	是	是	是	没有	是	没有	是
AWS::Amplify::Branch	是	是	是	是	没有	是	没有	是
AWS::ApiGateway::DomainName	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::ApiGateway::Method	是	是	是	是	是	是	是	是
AWS::ApiGateway::RestApi	是	是	是	是	是	是	是	是
AWS::ApiGateway::Stage	是	是	是	是	是	是	是	是
AWS::ApiGateway::UsagePlan	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Api	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Integration	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Stage	是	是	是	是	是	是	是	是
AWS::AppConfig::Application	是	是	是	是	没有	是	没有	是
AWS::AppConfig::ConfigurationProfile	是	是	是	是	没有	是	没有	是
AWS::AppConfig::DeploymentStrategy	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::AppConfig::Environment	是	是	是	是	没有	是	没有	是
AWS::AppConfig::Extension	是	是	是	是	是	是	是	是
AWS::AppConfig::ExtensionAssociation	是	是	是	是	是	是	是	是
AWS::AppConfig::HostedConfiguration版本	是	是	是	是	没有	是	没有	是
AWS::AppFlow::Flow	是	是	是	是	没有	是	没有	是
AWS::AppIntegrations::Application	没有	是	是	没有	没有	是	没有	没有
AWS::AppIntegrations::DataIntegration	没有	是	是	没有	没有	是	没有	没有
AWS::AppIntegrations::EventIntegration	没有	是	是	没有	没有	是	没有	没有
AWS::AppMesh::GatewayRoute	是	是	是	是	没有	是	没有	是
AWS::AppMesh::Mesh	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::AppMesh::Route	是	是	是	是	没有	是	没有	是
AWS::AppMesh::VirtualGateway	是	是	是	是	没有	是	没有	是
AWS::AppMesh::VirtualNode	是	是	是	是	没有	是	没有	是
AWS::AppMesh::VirtualRouter	是	是	是	是	没有	是	没有	是
AWS::AppMesh::VirtualService	是	是	是	是	没有	是	没有	是
AWS::AppRunner::Service	没有	是	是	是	没有	没有	没有	没有
AWS::AppRunner::VpcConnector	没有	是	是	是	没有	没有	没有	没有
AWS::AppStream::AppBlock生成器	没有	是	是	是	没有	是	没有	是
AWS::AppStream::Application	没有	是	是	是	没有	是	没有	是
AWS::AppStream::DirectoryConfig	没有	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::AppStream::Fleet	没有	是	是	是	没有	是	没有	没有
AWS::AppStream::Stack	没有	是	是	是	没有	是	没有	没有
AWS::AppSync::Api	是	是	是	是	是	是	没有	是
AWS::AppSync::ApiCache	是	是	是	是	没有	是	没有	是
AWS::AppSync::GraphQLApi	是	是	是	是	没有	是	没有	是
AWS::Athena::DataCatalog	是	是	是	是	是	是	是	是
AWS::Athena::PreparedStatement	是	是	是	是	是	是	是	是
AWS::Athena::WorkGroup	是	是	是	是	是	是	是	是
AWS::AuditManager::Assessment	是	是	是	是	没有	是	没有	没有
AWS::AutoScaling::AutoScaling群组	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::AutoScaling::LaunchConfiguration	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScalingPolicy	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScheduledAction	是	是	是	是	是	是	是	是
AWS::AutoScaling::WarmPool	是	是	是	是	没有	是	是	是
AWS::B2BI::Capability	没有	是	是	是	没有	没有	没有	没有
AWS::B2BI::Profile	没有	是	是	是	没有	没有	没有	没有
AWS::BCMDataExports::Export	没有	是	没有	没有	没有	没有	没有	没有
AWS::Backup::BackupPlan	是	是	是	是	是	是	是	是
AWS::Backup::BackupSelection	是	是	是	是	是	是	是	是
AWS::Backup::BackupVault	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Backup::RecoveryPoint	是	是	是	是	是	是	没有	是
AWS::Backup::ReportPlan	是	是	是	是	没有	是	没有	是
AWS::Backup::RestoreTesting计划	是	是	是	是	没有	是	没有	是
AWS::BackupGateway::Hypervisor	是	是	是	是	没有	是	没有	是
AWS::Batch::ComputeEnvironment	是	是	是	是	没有	是	没有	是
AWS::Batch::JobQueue	是	是	是	是	没有	是	没有	是
AWS::Batch::SchedulingPolicy	是	是	是	是	是	是	是	是
AWS::Bedrock::ApplicationInference 配置文件	没有	是	是	是	没有	是	没有	是
AWS::Bedrock::Guardrail	没有	是	是	是	没有	是	没有	是
AWS::Bedrock::KnowledgeBase	没有	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Bedrock::Prompt	没有	是	是	是	没有	是	没有	是
AWS::BedrockAgentCore::BrowserCustom	没有	是	是	是	没有	没有	没有	没有
AWS::BedrockAgentCore::CodeInterpreter自定义	没有	是	是	是	没有	没有	没有	没有
AWS::BedrockAgentCore::Runtime	没有	是	是	是	没有	没有	没有	没有
AWS::Budgets::BudgetsAction	没有	是	没有	没有	没有	没有	没有	没有
AWS::Cassandra::Keyspace	是	是	是	是	没有	是	没有	是
AWS::CleanRoomsML::TrainingDataset	没有	是	是	是	没有	没有	没有	没有
AWS::Cloud9::EnvironmentEC2	是	是	是	是	没有	是	没有	是
AWS::CloudFormation::GuardHook	是	是	是	是	是	是	是	是
AWS::CloudFormation::LambdaHook	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::CloudFormation::Stack	是	是	是	是	是	是	是	是
AWS::CloudFormation::StackSet	是	是	是	是	是	是	是	是
AWS::CloudFront::Distribution	没有	是	没有	没有	没有	没有	没有	没有
AWS::CloudFront::KeyValue存储	没有	是	没有	没有	没有	没有	没有	没有
AWS::CloudFront::PublicKey	没有	是	没有	没有	没有	没有	没有	没有
AWS::CloudFront::RealtimeLogConfig	没有	是	没有	没有	没有	没有	没有	没有
AWS::CloudFront::StreamingDistribution	没有	是	没有	没有	没有	没有	没有	没有
AWS::CloudTrail::EventData存储	是	是	是	是	没有	是	没有	是
AWS::CloudTrail::Trail	是	是	是	是	是	是	是	是
AWS::CloudWatch::Alarm	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::CloudWatch::MetricStream	是	是	是	是	没有	是	没有	是
AWS::CodeArtifact::Domain	没有	是	是	是	没有	没有	没有	没有
AWS::CodeArtifact::Repository	没有	是	是	是	没有	没有	没有	没有
AWS::CodeBuild::Project	是	是	是	是	没有	是	没有	是
AWS::CodeBuild::ReportGroup	是	是	是	是	没有	是	没有	是
AWS::CodeDeploy::Application	是	是	是	是	没有	是	没有	是
AWS::CodeDeploy::DeploymentConfig	是	是	是	是	没有	是	没有	是
AWS::CodeDeploy::DeploymentGroup	是	是	是	是	没有	是	没有	是
AWS::CodeGuruProfiler::ProfilingGroup	没有	是	是	是	没有	没有	没有	没有
AWS::CodeGuruReviewer::RepositoryAssociation	没有	是	是	是	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::CodePipeline::Pipeline	是	是	是	是	没有	是	没有	是
AWS::Cognito::IdentityPool	是	是	是	是	是	是	是	是
AWS::Cognito::UserPool	是	是	是	是	是	是	是	是
AWS::Cognito::UserPool客户端	是	是	是	是	是	是	是	是
AWS::Cognito::UserPool群组	是	是	是	是	是	是	是	是
AWS::Comprehend::Flywheel	没有	是	是	是	没有	是	没有	没有
AWS::Config::AggregationAuthorization	是	是	是	是	是	是	是	是
AWS::Config::ConfigurationRecorder	是	是	是	是	是	是	是	是
AWS::Config::ConformancePack	是	是	是	是	是	是	没有	是
AWS::Config::ConformancePack Compliance	是	是	是	是	是	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Config::ResourceCompliance	是	是	是	是	是	是	是	是
AWS::Config::StoredQuery	是	是	是	是	是	是	是	是
AWS::Connect::Instance	没有	是	是	没有	没有	是	没有	没有
AWS::Connect::PhoneNumber	没有	是	是	没有	没有	是	没有	没有
AWS::Connect::QuickConnect	没有	是	是	没有	没有	是	没有	没有
AWS::Connect::Rule	没有	是	是	没有	没有	是	没有	没有
AWS::Connect::SecurityProfile	没有	是	是	没有	没有	是	没有	没有
AWS::Connect::User	没有	是	是	没有	没有	是	没有	没有
AWS::CustomerProfiles::Domain	没有	是	是	没有	没有	是	没有	没有
AWS::CustomerProfiles::ObjectType	没有	是	是	没有	没有	是	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::DMS::Certificate	是	是	是	是	没有	是	没有	是
AWS::DMS::Endpoint	是	是	是	是	没有	是	没有	是
AWS::DMS::EventSubscription	是	是	是	是	没有	是	没有	是
AWS::DMS::MigrationProject	是	是	是	是	是	是	没有	是
AWS::DMS::ReplicationInstance	是	是	是	是	没有	是	没有	是
AWS::DMS::ReplicationSubnet群组	是	是	是	是	没有	是	没有	是
AWS::DMS::ReplicationTask	是	是	是	是	没有	是	没有	是
AWS::DataSync::Agent	是	是	是	是	是	是	是	是
AWS::DataSync::LocationEFS	是	是	是	是	没有	是	没有	是
AWS::DataSync::LocationFSxLustre	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::DataSync::LocationFSx窗户	是	是	是	是	没有	是	没有	是
AWS::DataSync::LocationHDFS	是	是	是	是	没有	是	是	是
AWS::DataSync::LocationNFS	是	是	是	是	没有	是	是	是
AWS::DataSync::LocationObject存储	是	是	是	是	没有	是	是	是
AWS::DataSync::LocationS3	是	是	是	是	是	是	是	是
AWS::DataSync::Location中小型企业	是	是	是	是	没有	是	是	是
AWS::DataSync::Task	是	是	是	是	是	是	是	是
AWS::Deadline::Fleet	没有	是	是	是	没有	没有	没有	没有
AWS::Deadline::Monitor	没有	是	是	是	没有	没有	没有	没有
AWS::Deadline::QueueFleet协会	没有	是	是	是	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Detective::Graph	是	是	是	是	没有	是	没有	是
AWS::DeviceFarm::InstanceProfile	没有	没有	是	没有	没有	没有	没有	没有
AWS::DeviceFarm::Project	没有	没有	是	没有	没有	没有	没有	没有
AWS::DeviceFarm::TestGrid项目	没有	没有	是	没有	没有	没有	没有	没有
AWS::DynamoDB::Table	是	是	是	是	是	是	是	是
AWS::EC2::CapacityReservation	是	是	是	是	是	是	没有	是
AWS::EC2::CarrierGateway	没有	是	是	是	没有	是	没有	没有
AWS::EC2::ClientVpn端点	是	是	是	是	没有	是	没有	是
AWS::EC2::ClientVpnTargetNetworkAssociation	是	是	是	是	没有	是	没有	是
AWS::EC2::CustomerGateway	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS:EC2::: DHCPOptions	是	是	是	是	是	是	是	是
AWS:EC2:: EC2 舰队	是	是	是	是	没有	是	没有	是
AWS:::EC2: EIP	是	是	是	是	是	是	是	是
AWS:EC2::: EIPAssociation	是	是	是	是	是	是	是	是
AWS::EC2::EgressOnlyInternetGateway	是	是	是	是	没有	是	没有	是
AWS::EC2::FlowLog	是	是	是	是	是	是	是	是
AWS::EC2::Host	是	是	是	是	是	是	是	是
AWS:::EC2: IPAM	是	是	是	是	没有	是	没有	是
AWS:EC2::: IPAMPool	是	是	是	是	没有	是	没有	是
AWS::EC2:: IPAMPool Cidr	是	是	是	是	是	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::EC2: IPAMResource Discovery	是	是	是	是	没有	是	没有	是
AWS:EC2::: IPAMResource DiscoveryAssociation	是	是	是	是	没有	是	没有	是
AWS:EC2::: IPAMScope	是	是	是	是	没有	是	没有	是
AWS::EC2::Instance	是	是	是	是	是	是	是	是
AWS::EC2::Instance Connect端点	是	是	是	是	是	是	是	是
AWS::EC2: :InternetGateway	是	是	是	是	是	是	是	是
AWS::EC2: :LaunchTemplate	是	是	是	是	没有	是	没有	是
AWS::EC2::NatGateway	是	是	是	是	没有	是	没有	是
AWS::EC2::NetworkAcl	是	是	是	是	是	是	是	是
AWS::EC2::NetworkInsightsAccessScope	是	是	是	是	没有	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::EC2::NetworkInsightsAccessScopeAnalysis	是	是	是	是	没有	是	是	是
AWS::EC2::NetworkInsights分析	是	是	是	是	没有	是	没有	是
AWS::EC2::NetworkInsights路径	是	是	是	是	没有	是	是	是
AWS::EC2::NetworkInterface	是	是	是	是	是	是	是	是
AWS::EC2::PrefixList	是	是	是	是	是	是	是	是
AWS::EC2::RouteTable	是	是	是	是	是	是	是	是
AWS::EC2::SecurityGroup	是	是	是	是	是	是	是	是
AWS::EC2::SecurityGroupVpcAssociation	是	是	是	是	是	是	是	是
AWS::EC2::SnapshotBlockPublicAccess	是	是	是	是	是	是	是	是
AWS::EC2::SpotFleet	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::EC2::Subnet	是	是	是	是	是	是	是	是
AWS::EC2::SubnetCidr屏蔽	是	是	是	是	是	是	是	是
AWS::EC2::SubnetNetworkAclAssociation	是	是	是	是	没有	是	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是	是	是	没有	是	是	是
AWS::EC2::TrafficMirror过滤器	是	是	是	是	是	是	是	是
AWS::EC2::TrafficMirrorSession	是	是	是	是	没有	是	是	是
AWS::EC2::TrafficMirror目标	是	是	是	是	没有	是	是	是
AWS::EC2::TransitGateway	是	是	是	是	是	是	是	是
AWS::EC2::TransitGateway附件	是	是	是	是	没有	是	没有	是
AWS::EC2::TransitGatewayConnect	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::EC2::TransitGatewayMulticastDomain	是	是	是	是	是	是	是	是
AWS::EC2::TransitGatewayRouteTable	是	是	是	是	没有	是	没有	是
AWS:::EC2: VPC	是	是	是	是	是	是	是	是
AWS:EC2::: VPCBlockPublicAccessExclusion	是	是	是	是	是	是	没有	是
AWS:EC2::: VPCBlockPublicAccessOptions	是	是	是	是	是	是	没有	是
AWS:EC2::: VPCEndpoint	是	是	是	是	是	是	是	是
AWS:EC2::: VPCEndpoint ConnectionNotification	是	是	是	是	是	是	是	是
AWS:EC2::: VPCEndpoint 服务	是	是	是	是	是	是	是	是
AWS::EC2:: VPCGateway 附件	是	是	是	是	是	是	是	是
AWS:EC2:: VPCPeering 连接	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS:EC2::: VPNConnection	是	是	是	是	是	是	是	是
AWS::EC2:: VPNConnection 路线	是	是	是	是	是	是	是	是
AWS:EC2::: VPNGateway	是	是	是	是	是	是	是	是
AWS::EC2::Verified Access实例	是	是	是	是	没有	是	没有	是
AWS::EC2::Volume	是	是	是	是	是	是	是	是
AWS::ECR: :PublicRepository	没有	是	没有	没有	没有	没有	没有	没有
AWS::ECR::PullThroughCacheRule	是	是	是	是	是	是	是	是
AWS::ECR::RegistryPolicy	是	是	是	是	是	是	是	是
AWS::ECR::ReplicationConfiguration	是	是	是	是	是	是	是	是
AWS::ECR::Repository	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::ECR::RepositoryCreation模板	是	是	是	是	是	是	是	是
AWS::ECS::CapacityProvider	是	是	是	是	是	是	是	是
AWS::ECS::Cluster	是	是	是	是	是	是	是	是
AWS::ECS::Service	是	是	是	是	是	是	是	是
AWS::ECS::TaskDefinition	是	是	是	是	是	是	是	是
AWS::ECS::TaskSet	是	是	是	是	没有	是	没有	是
AWS::EFS::AccessPoint	是	是	是	是	是	是	是	是
AWS::EFS::FileSystem	是	是	是	是	是	是	是	是
AWS::EKS::Addon	是	是	是	是	没有	是	没有	是
AWS::EKS::Cluster	是	是	是	是	没有	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::EKS::FargateProfile	是	是	是	是	没有	是	没有	是
AWS::EKS::IdentityProviderConfig	是	是	是	是	没有	是	没有	是
AWS::EMR::SecurityConfiguration	是	是	是	是	是	是	是	是
AWS::EMR::Studio	是	是	是	是	是	是	没有	是
AWS::EMRContainers::VirtualCluster	是	是	是	是	没有	是	没有	是
AWS::EMRServerless::Application	是	是	是	是	没有	是	没有	是
AWS::ElasticBeanstalk::Application	是	是	是	是	是	是	没有	是
AWS::ElasticBeanstalk::ApplicationVersion	是	是	是	是	是	是	没有	是
AWS::ElasticBeanstalk::Environment	是	是	是	是	是	是	没有	是
AWS::ElasticLoadBalancing::LoadBalancer	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::ElasticLoadBalancingV2::Listener	是	是	是	是	没有	是	是	是
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是	是	是	是	是	是	是
AWS::ElasticLoadBalancingV2::TargetGroup	是	是	是	是	是	是	是	是
AWS::Elasticsearch::Domain	是	是	是	是	是	是	是	是
AWS::EntityResolution::IdMapping工作流程	没有	是	是	是	没有	是	没有	没有
AWS::EntityResolution::MatchingWorkflow	没有	是	是	是	没有	是	没有	没有
AWS::EntityResolution::SchemaMapping	没有	是	是	是	没有	是	没有	没有
AWS::EventSchemas::Discoverer	是	是	是	是	没有	是	没有	是
AWS::EventSchemas::Registry	是	是	是	是	没有	是	没有	是
AWS::EventSchemas::RegistryPolicy	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::EventSchemas::Schema	是	是	是	是	没有	是	没有	是
AWS::Events::ApiDestination	是	是	是	是	没有	是	没有	是
AWS::Events::Archive	是	是	是	是	没有	是	没有	是
AWS::Events::Connection	是	是	是	是	没有	是	没有	是
AWS::Events::Endpoint	是	是	是	是	没有	是	没有	是
AWS::Events::EventBus	是	是	是	是	是	是	是	是
AWS::Events::Rule	是	是	是	是	没有	是	没有	是
AWS::FIS::ExperimentTemplate	是	是	是	是	没有	是	没有	是
AWS::Forecast::Dataset	没有	是	是	是	没有	没有	没有	没有
AWS::Forecast::DatasetGroup	没有	是	是	是	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::FraudDetector::EntityType	没有	是	是	是	没有	没有	没有	没有
AWS::FraudDetector::Label	没有	是	是	是	没有	没有	没有	没有
AWS::FraudDetector::Outcome	没有	是	是	是	没有	没有	没有	没有
AWS::FraudDetector::Variable	没有	是	是	是	没有	没有	没有	没有
AWS::GameLift::Alias	是	是	是	是	没有	是	没有	是
AWS::GameLift::Build	是	是	是	是	没有	是	没有	是
AWS::GameLift::GameSession队列	是	是	是	是	没有	是	没有	是
AWS::GameLift::MatchmakingConfiguration	没有	是	是	没有	没有	没有	没有	没有
AWS::GlobalAccelerator::Accelerator	没有	没有	是	没有	没有	没有	没有	没有
AWS::GlobalAccelerator::EndpointGroup	没有	没有	是	没有	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::GlobalAccelerator::Listener	没有	没有	是	没有	没有	没有	没有	没有
AWS::Glue::Classifier	是	是	是	是	是	是	是	是
AWS::Glue::Database	是	是	是	是	没有	是	没有	是
AWS::Glue::Job	是	是	是	是	是	是	没有	是
AWS::Glue::MLTransform	是	是	是	是	是	是	是	是
AWS::Glue::Registry	是	是	是	是	没有	是	没有	是
AWS::Grafana::Workspace	没有	是	是	是	没有	没有	没有	没有
AWS::GreengrassV2::ComponentVersion	没有	是	是	是	没有	是	没有	没有
AWS::GroundStation::Config	没有	是	是	是	没有	没有	没有	是
AWS::GroundStation::DataflowEndpoint群组	没有	是	是	是	没有	没有	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::GroundStation::MissionProfile	没有	是	是	是	没有	没有	没有	是
AWS::GuardDuty::Detector	是	是	是	是	是	是	是	是
AWS::GuardDuty::Filter	是	是	是	是	没有	是	没有	是
AWS::Guard职责:: IPSet	是	是	是	是	没有	是	是	是
AWS::GuardDuty::MalwareProtection计划	是	是	是	是	是	是	没有	是
AWS::GuardDuty::ThreatIntelSet	是	是	是	是	没有	是	是	是
AWS::Health湖::FHIRDatastore	没有	是	是	是	没有	没有	没有	没有
AWS::IAM::Group	是	是	是	是	没有	是	没有	是
AWS::IAM::InstanceProfile	没有	是	没有	没有	没有	没有	没有	没有
AWS:: IAM:: OIDCProvider	没有	是	没有	没有	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::IAM::Policy	是	是	是	是	没有	是	没有	是
AWS::IAM::Role	是	是	是	是	没有	是	没有	是
AWS:: IAM:: SAMLProvider	没有	是	没有	没有	没有	没有	没有	没有
AWS::IAM::ServerCertificate	没有	是	没有	没有	没有	没有	没有	没有
AWS::IAM::User	是	是	是	是	没有	是	没有	是
AWS::IVS::Channel	没有	是	是	没有	没有	没有	没有	没有
AWS::IVS::PlaybackKey配对	没有	是	是	没有	没有	没有	没有	没有
AWS::IVS::RecordingConfiguration	没有	是	是	没有	没有	没有	没有	没有
AWS::ImageBuilder::ContainerRecipe	是	是	是	是	是	是	是	是
AWS::ImageBuilder::DistributionConfiguration	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::ImageBuilder::ImagePipeline	是	是	是	是	是	是	是	是
AWS::ImageBuilder::ImageRecipe	是	是	是	是	是	是	是	是
AWS::ImageBuilder::InfrastructureConfiguration	是	是	是	是	没有	是	没有	是
AWS::ImageBuilder::LifecyclePolicy	是	是	是	是	没有	是	没有	是
AWS::InspectorV2::Activation	是	是	是	是	是	是	是	是
AWS::InspectorV2::Filter	是	是	是	是	没有	是	是	是
AWS::IoT::AccountAudit配置	是	是	是	是	没有	是	没有	没有
AWS::IoT::Authorizer	是	是	是	是	没有	是	没有	是
AWS::IoT:: CACertificate	是	是	是	是	没有	是	没有	是
AWS::IoT::CustomMetric	是	是	是	是	没有	是	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::IoT::Dimension	是	是	是	是	没有	是	没有	没有
AWS::IoT::DomainConfiguration	是	是	是	是	没有	是	没有	是
AWS::IoT::FleetMetric	是	是	是	是	没有	是	没有	是
AWS::IoT::JobTemplate	是	是	是	是	没有	是	没有	是
AWS::IoT::MitigationAction	是	是	是	是	没有	是	没有	没有
AWS::IoT::Policy	是	是	是	是	没有	是	没有	是
AWS::IoT::ProvisioningTemplate	是	是	是	是	没有	是	没有	是
AWS::IoT::RoleAlias	是	是	是	是	没有	是	没有	是
AWS::IoT::ScheduledAudit	是	是	是	是	没有	是	没有	没有
AWS::IoT::SecurityProfile	是	是	是	是	没有	是	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::IoT::ThingGroup	是	是	是	是	没有	是	没有	是
AWS::IoTAnalytics::Channel	没有	是	是	是	没有	没有	没有	没有
AWS::IoTAnalytics::Dataset	没有	是	是	是	没有	没有	没有	没有
AWS::IoTAnalytics::Datastore	没有	是	是	是	没有	没有	没有	没有
AWS::IoTAnalytics::Pipeline	没有	是	是	是	没有	没有	没有	没有
AWS::IoTCoreDeviceAdvisor::SuiteDefinition	没有	是	是	没有	没有	没有	没有	没有
AWS::IoTEvents::AlarmModel	没有	是	是	是	没有	是	没有	没有
AWS::IoTEvents::DetectorModel	没有	是	是	是	没有	是	没有	没有
AWS::IoTEvents::Input	没有	是	是	是	没有	是	没有	没有
AWS::IoTSiteWise::Asset	没有	是	是	是	没有	是	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::IoTSiteWise::AssetModel	没有	是	是	是	没有	是	没有	没有
AWS::IoTSiteWise::Dashboard	没有	是	是	是	没有	是	没有	没有
AWS::IoTSiteWise::Gateway	没有	是	是	是	没有	是	没有	没有
AWS::IoTSiteWise::Portal	没有	是	是	是	没有	是	没有	没有
AWS::IoTSiteWise::Project	没有	是	是	是	没有	是	没有	没有
AWS::IoTTwinMaker::ComponentType	没有	是	是	没有	没有	没有	没有	没有
AWS::IoTTwinMaker::Entity	没有	是	是	没有	没有	没有	没有	没有
AWS::IoTTwinMaker::Scene	没有	是	是	没有	没有	没有	没有	没有
AWS::IoTTwinMaker::SyncJob	没有	是	是	没有	没有	没有	没有	没有
AWS::IoTTwinMaker::Workspace	没有	是	是	没有	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::IoTWireless::FuotaTask	没有	是	是	没有	没有	没有	没有	是
AWS::IoTWireless::MulticastGroup	没有	是	是	没有	没有	没有	没有	是
AWS::IoTWireless::ServiceProfile	没有	是	是	没有	没有	没有	没有	是
AWS::KMS::Alias	是	是	是	是	没有	是	是	是
AWS::KMS::Key	是	是	是	是	是	是	是	是
AWS::KafkaConnect::Connector	是	是	是	是	没有	是	没有	是
AWS::KafkaConnect::CustomPlugin	是	是	是	是	没有	是	是	是
AWS::Kendra::Index	没有	是	是	是	没有	是	没有	没有
AWS::Kinesis::Stream	是	是	是	是	没有	是	是	是
AWS::Kinesis::StreamConsumer	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::KinesisAnalyticsV2::Application	是	是	是	是	是	是	是	是
AWS::KinesisFirehose::DeliveryStream	是	是	是	是	没有	是	是	是
AWS::KinesisVideo::SignalingChannel	没有	是	是	是	没有	是	没有	是
AWS::KinesisVideo::Stream	没有	是	是	是	没有	是	没有	是
AWS::Lambda::CodeSigningConfig	是	是	是	是	没有	是	没有	是
AWS::Lambda::Function	是	是	是	是	是	是	是	是
AWS::Lex::Bot	没有	是	是	没有	没有	是	没有	没有
AWS::Lex::BotAlias	没有	是	是	没有	没有	是	没有	没有
AWS::Lightsail::Bucket	没有	是	是	是	没有	是	没有	没有
AWS::Lightsail::Certificate	没有	是	是	是	没有	是	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Lightsail::Disk	没有	是	是	是	没有	是	没有	没有
AWS::Lightsail::StaticIp	没有	是	是	是	没有	是	没有	没有
AWS::Location::APIKey	没有	是	是	是	没有	是	没有	是
AWS::Location::GeofenceCollection	没有	是	是	是	没有	是	没有	是
AWS::Location::Map	没有	是	是	是	没有	是	没有	是
AWS::Location::PlaceIndex	没有	是	是	是	没有	是	没有	是
AWS::Location::RouteCalculator	没有	是	是	是	没有	是	没有	是
AWS::Logs::Destination	是	是	是	是	是	是	是	是
AWS::LookoutVision::Project	没有	是	是	是	没有	没有	没有	没有
AWS::M2::Environment	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::MSK::BatchScram秘密	是	是	是	是	没有	是	没有	是
AWS::MSK::Cluster	是	是	是	是	没有	是	没有	是
AWS::MSK::ClusterPolicy	是	是	是	是	没有	是	没有	是
AWS::MSK::Configuration	是	是	是	是	是	是	是	是
AWS::MSK::ServerlessCluster	没有	是	是	是	没有	是	没有	没有
AWS::MSK::VpcConnection	是	是	是	是	没有	是	没有	是
AWS::Macie::Session	是	是	是	是	没有	是	没有	是
AWS::MediaConnect::FlowEntitlement	是	是	是	是	没有	是	没有	是
AWS::MediaConnect::FlowSource	是	是	是	是	没有	是	没有	是
AWS::MediaConnect::FlowVpc接口	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::MediaConnect::Gateway	是	是	是	是	没有	是	没有	是
AWS::MediaLive::Multiplexprogram	没有	是	是	是	没有	是	没有	是
AWS::MediaPackage::Asset	是	是	是	是	没有	是	没有	是
AWS::MediaPackage::PackagingConfiguration	是	是	是	是	没有	是	没有	是
AWS::MediaPackage::PackagingGroup	是	是	是	是	没有	是	没有	是
AWS::MediaPackageV2::Channel	是	是	是	是	没有	是	没有	是
AWS::MediaPackageV2::ChannelGroup	是	是	是	是	没有	是	没有	是
AWS::MediaPackageV2::OriginEndpoint	是	是	是	是	没有	是	没有	是
AWS::MediaTailor::LiveSource	没有	是	是	是	没有	是	没有	是
AWS::MediaTailor::PlaybackConfiguration	没有	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::MemoryDB::SubnetGroup	是	是	是	是	没有	是	没有	是
AWS::NetworkFirewall::Firewall	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::RuleGroup	是	是	是	是	是	是	是	是
AWS::Network防火墙:: TLSInspection 配置	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::VpcEndpoint协会	是	是	是	是	是	是	是	是
AWS::NetworkManager::ConnectPeer	没有	没有	是	没有	没有	没有	没有	没有
AWS::NetworkManager::CustomerGateway协会	没有	没有	是	没有	没有	没有	没有	没有
AWS::NetworkManager::Device	没有	没有	是	没有	没有	没有	没有	没有
AWS::NetworkManager::GlobalNetwork	没有	没有	是	没有	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::NetworkManager::Link	没有	没有	是	没有	没有	没有	没有	没有
AWS::NetworkManager::LinkAssociation	没有	没有	是	没有	没有	没有	没有	没有
AWS::NetworkManager::Site	没有	没有	是	没有	没有	没有	没有	没有
AWS::NetworkManager::TransitGateway对等	没有	没有	是	没有	没有	没有	没有	没有
AWS::NetworkManager::TransitGateway注册	没有	没有	是	没有	没有	没有	没有	没有
AWS::Omics::RunGroup	没有	是	是	没有	没有	没有	没有	没有
AWS::Omics::Workflow	没有	是	是	没有	没有	没有	没有	没有
AWS::OpenSearch::Domain	是	是	是	是	没有	是	没有	是
AWS::OpenSearchServerless::Collection	没有	是	是	是	没有	是	没有	是
AWS::OpenSearchServerless::SecurityConfig	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::OpenSearchServerless::VpcEndpoint	没有	是	是	是	没有	是	没有	是
AWS::PCAConnectorAD::Connector	是	是	是	是	是	是	是	是
AWS::PCAConnectorAD::DirectoryRegistration	是	是	是	是	是	是	是	是
AWS::Panorama::Package	没有	是	是	没有	没有	是	没有	没有
AWS::Personalize::Dataset	没有	是	是	是	没有	是	没有	没有
AWS::Personalize::DatasetGroup	没有	是	是	是	没有	是	没有	没有
AWS::Personalize::Schema	没有	是	是	是	没有	是	没有	没有
AWS::Personalize::Solution	没有	是	是	是	没有	是	没有	没有
AWS::Pinpoint::App	没有	是	是	没有	没有	是	没有	没有
AWS::Pinpoint::ApplicationSettings	没有	是	是	没有	没有	是	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Pinpoint::Campaign	没有	是	是	没有	没有	是	没有	没有
AWS::Pinpoint::EmailChannel	没有	是	是	没有	没有	是	没有	没有
AWS::Pinpoint::EmailTemplate	没有	是	是	没有	没有	是	没有	没有
AWS::Pinpoint::EventStream	没有	是	是	没有	没有	是	没有	没有
AWS::Pinpoint::InApp模板	没有	是	是	是	没有	是	没有	没有
AWS::Pinpoint::Segment	没有	是	是	没有	没有	是	没有	没有
AWS::QuickSight::Dashboard	没有	是	是	是	没有	是	没有	是
AWS::QuickSight::DataSource	没有	是	是	是	没有	是	没有	是
AWS::QuickSight::Template	没有	是	是	是	没有	是	没有	是
AWS::QuickSight::Theme	没有	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS:: RDS:: DBCluster	是	是	是	是	是	是	是	是
AWS:: RDS:: 快照 DBCluster	是	是	是	是	是	是	是	是
AWS:: RDS:: DBInstance	是	是	是	是	是	是	是	是
AWS:: RDS:: 终端节点 DBProxy	是	是	是	是	是	是	是	是
AWS:: RDS:: 群组 DBSecurity	是	是	是	是	是	是	是	是
AWS:: RDS:: DBSnapshot	是	是	是	是	是	是	是	是
AWS:: RDS:: 群组 DBSubnet	是	是	是	是	是	是	是	是
AWS::RDS::EventSubscription	是	是	是	是	是	是	是	是
AWS::RDS::GlobalCluster	是	是	是	是	没有	是	是	是
AWS::RDS::Integration	是	是	是	是	是	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::RDS::OptionGroup	是	是	是	是	是	是	没有	是
AWS::RUM::AppMonitor	是	是	是	是	没有	是	没有	是
AWS::Redshift::Cluster	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterParameter群组	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSecurity群组	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSnapshot	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSubnet群组	是	是	是	是	是	是	是	是
AWS::Redshift::EndpointAccess	是	是	是	是	没有	是	没有	是
AWS::Redshift::EndpointAuthorization	是	是	是	是	没有	是	没有	是
AWS::Redshift::EventSubscription	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Redshift::Integration	是	是	是	是	是	是	是	是
AWS::Redshift::ScheduledAction	是	是	是	是	没有	是	没有	是
AWS::ResilienceHub::App	是	是	是	是	没有	是	没有	是
AWS::ResilienceHub::ResiliencyPolicy	是	是	是	是	没有	是	没有	是
AWS::ResourceExplorer2::Index	是	是	是	是	是	是	是	是
AWS::RoboMaker::RobotApplication	没有	是	是	是	没有	没有	没有	没有
AWS::RoboMaker::RobotApplication版本	没有	是	是	是	没有	没有	没有	没有
AWS::RoboMaker::SimulationApplication	没有	是	是	是	没有	没有	没有	没有
AWS::Roles任何地方:: CRL	是	是	是	是	是	是	是	是
AWS::RolesAnywhere::Profile	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::RolesAnywhere::TrustAnchor	是	是	是	是	是	是	是	是
AWS::Route53:: DNSSEC	没有	是	没有	没有	没有	没有	没有	没有
AWS::Route53::HealthCheck	没有	是	没有	没有	没有	没有	没有	没有
AWS::Route53::HostedZone	没有	是	没有	没有	没有	没有	没有	没有
AWS::Route53Profiles::Profile	是	是	是	是	是	是	是	是
AWS::Route53Profiles::ProfileAssociation	是	是	是	是	是	是	是	是
AWS::Route53RecoveryControl::Cluster	没有	没有	是	没有	没有	没有	没有	没有
AWS::Route53RecoveryControl::ControlPanel	没有	没有	是	没有	没有	没有	没有	没有
AWS::Route53RecoveryControl::RoutingControl	没有	没有	是	没有	没有	没有	没有	没有
AWS::Route53RecoveryControl::SafetyRule	没有	没有	是	没有	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Route53RecoveryReadiness::Cell	没有	没有	是	没有	没有	没有	没有	没有
AWS::Route53RecoveryReadiness::ReadinessCheck	没有	没有	是	没有	没有	没有	没有	没有
AWS::Route53RecoveryReadiness::RecoveryGroup	没有	没有	是	没有	没有	没有	没有	没有
AWS::Route53RecoveryReadiness::ResourceSet	没有	没有	是	没有	没有	没有	没有	没有
AWS::Route53Resolver::FirewallDomain名单	是	是	是	是	没有	是	没有	是
AWS::Route53Resolver::FirewallRule群组	是	是	是	是	没有	是	没有	是
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverEndpoint	是	是	是	是	没有	是	没有	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverRule	是	是	是	是	没有	是	没有	是
AWS::Route53Resolver::ResolverRule协会	是	是	是	是	没有	是	没有	是
AWS::S3::AccessGrant	是	是	是	是	是	是	是	是
AWS::S3::AccessGrants实例	是	是	是	是	是	是	是	是
AWS::S3::AccessGrantsLocation	是	是	是	是	是	是	是	是
AWS::S3::AccessPoint	是	是	是	是	没有	是	是	是
AWS::S3::AccountPublicAccessBlock	是	是	是	是	没有	是	没有	是
AWS::S3::Bucket	是	是	是	是	是	是	是	是
AWS::S3::MultiRegionAccessPoint	没有	没有	是	没有	没有	没有	没有	没有

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::S3::StorageLens	是	是	是	是	没有	是	没有	是
AWS::S3::StorageLens群组	是	是	是	是	没有	是	没有	是
AWS::S3Express::BucketPolicy	没有	是	是	是	没有	没有	没有	没有
AWS::S3Express::DirectoryBucket	没有	是	是	是	没有	没有	没有	没有
AWS::S3Tables::TableBucket	是	是	是	是	是	是	是	是
AWS::S3Tables::TableBucket政策	是	是	是	是	是	是	是	是
AWS::SES::ConfigurationSet	是	是	是	是	没有	是	没有	是
AWS::SES::ContactList	是	是	是	是	没有	是	没有	是
AWS::SES::DedicatedIp泳池	是	是	是	是	没有	是	没有	是
AWS::SES::MailManagerTrafficPolicy	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::SES::ReceiptFilter	没有	是	是	是	没有	是	没有	是
AWS::SES::ReceiptRuleSet	没有	是	是	是	没有	是	没有	是
AWS::SES::Template	是	是	是	是	没有	是	没有	是
AWS::SNS::Topic	是	是	是	是	是	是	是	是
AWS::SQS::Queue	是	是	是	是	没有	是	没有	是
AWS::SSM::AssociationCompliance	是	是	是	是	是	是	是	是
AWS::SSM::Document	是	是	是	是	是	是	是	是
AWS::SSM::FileData	是	是	是	是	是	是	是	是
AWS::SSM::ManagedInstance 清单	是	是	是	是	是	是	是	是
AWS::SSM::PatchCompliance	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::SSM::ResourceData同步	是	是	是	是	是	是	是	是
AWS::SSMContacts::Contact	是	是	是	是	没有	是	没有	是
AWS::SSMIncidents::ResponsePlan	是	是	是	是	没有	是	没有	是
AWS::SageMaker::AppImageConfig	是	是	是	是	没有	是	没有	是
AWS::SageMaker::CodeRepository	是	是	是	是	没有	是	没有	是
AWS::SageMaker::DataQualityJobDefinition	是	是	是	是	没有	是	没有	是
AWS::SageMaker::Domain	是	是	是	是	没有	是	没有	是
AWS::SageMaker::EndpointConfig	是	是	是	是	没有	是	没有	是
AWS::SageMaker::FeatureGroup	是	是	是	是	没有	是	没有	是
AWS::SageMaker::Image	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::SageMaker::InferenceExperiment	是	是	是	是	没有	是	没有	是
AWS::SageMaker::MlflowTracking服务器	是	是	是	是	是	是	是	是
AWS::SageMaker::Model	是	是	是	是	没有	是	没有	是
AWS::SageMaker::ModelBiasJobDefinition	是	是	是	是	没有	是	没有	是
AWS::SageMaker::ModelExplainabilityJobDefinition	是	是	是	是	没有	是	没有	是
AWS::SageMaker::ModelQualityJobDefinition	是	是	是	是	没有	是	没有	是
AWS::SageMaker::MonitoringSchedule	是	是	是	是	没有	是	没有	是
AWS::SageMaker::NotebookInstance	是	是	是	是	没有	是	没有	是
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	是	是	是	没有	是	没有	是
AWS::SageMaker::StudioLifecycleConfig	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::SageMaker::UserProfile	是	是	是	是	没有	是	没有	是
AWS::SageMaker::Workteam	没有	是	是	是	没有	是	没有	没有
AWS::SecretsManager::ResourcePolicy	是	是	是	是	是	是	是	是
AWS::SecretsManager::RotationSchedule	是	是	是	是	是	是	是	是
AWS::SecretsManager::Secret	是	是	是	是	是	是	是	是
AWS::SecurityHub::Standard	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::CloudFormation产品	是	是	是	是	没有	是	没有	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是	是	是	没有	是	没有	是
AWS::ServiceCatalog::Portfolio	是	是	是	是	没有	是	没有	是
AWS::ServiceDiscovery::HttpNamespace	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::ServiceDiscovery::Instance	是	是	是	是	没有	是	没有	是
AWS::ServiceDiscovery::PublicDns命名空间	是	是	是	是	是	是	是	是
AWS::ServiceDiscovery::Service	是	是	是	是	没有	是	是	是
AWS::Shield::Protection	没有	是	没有	没有	没有	没有	没有	没有
AWS::ShieldRegional::Protection	是	是	是	是	是	是	是	是
AWS::Signer::SigningProfile	是	是	是	是	没有	是	没有	是
AWS::StepFunctions::Activity	是	是	是	是	是	是	是	是
AWS::StepFunctions::StateMachine	是	是	是	是	是	是	是	是
AWS::Transfer::Agreement	是	是	是	是	没有	是	是	是
AWS::Transfer::Certificate	是	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::Transfer::Connector	是	是	是	是	是	是	是	是
AWS::Transfer::Profile	是	是	是	是	是	是	是	是
AWS::Transfer::Server	是	是	是	是	是	是	是	是
AWS::Transfer::Workflow	是	是	是	是	是	是	是	是
AWS::WAF::RateBased规则	没有	是	没有	没有	没有	没有	没有	没有
AWS::WAF::Rule	没有	是	没有	没有	没有	没有	没有	没有
AWS::WAF::RuleGroup	没有	是	没有	没有	没有	没有	没有	没有
AWS::WAF::WebACL	没有	是	没有	没有	没有	没有	没有	没有
AWS::WAFRegional::RateBased规则	是	是	是	是	没有	是	没有	是
AWS::WAFRegional::Rule	是	是	是	是	没有	是	没有	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	墨西哥（中部）	南美洲（圣保罗）
AWS::WAFRegional::RuleGroup	是	是	是	是	没有	是	没有	是
AWS::WAFRegional::WebACL	是	是	是	是	没有	是	没有	是
AWS:WAFv2::: IPSet	是	是	是	是	是	是	是	是
AWS::WAFv2::ManagedRuleSet	是	是	是	是	是	是	是	是
AWS::WAFv2::RegexPatternSet	是	是	是	是	是	是	是	是
AWS::WAFv2::RuleGroup	是	是	是	是	是	是	是	是
AWS::WAFv2::WebACL	是	是	是	是	是	是	是	是
AWS::WorkSpaces::ConnectionAlias	没有	是	是	没有	没有	是	没有	是
AWS::WorkSpaces::Workspace	没有	是	是	没有	没有	是	没有	是
AWS::XRay::EncryptionConfig	是	是	是	是	没有	是	是	是

欧洲区域

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ACM::Certificate	是	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority	是	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority激活	是	是	是	是	是	是	是	是
AWS::APS::RuleGroups命名空间	是	是	是	是	是	没有	没有	没有
AWS::AccessAnalyzer::Analyzer	是	是	是	是	是	是	是	是
AWS::AmazonMQ::Broker	是	是	是	是	是	是	没有	没有
AWS::Amplify::App	是	是	是	是	是	是	没有	没有
AWS::Amplify::Branch	是	是	是	是	是	是	没有	没有
AWS::ApiGateway::DomainName	是	是	是	是	是	是	是	是
AWS::ApiGateway::Method	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ApiGateway::RestApi	是	是	是	是	是	是	是	是
AWS::ApiGateway::Stage	是	是	是	是	是	是	是	是
AWS::ApiGateway::UsagePlan	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Api	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Integration	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Stage	是	是	是	是	是	是	是	是
AWS::AppConfig::Application	是	是	是	是	是	是	没有	没有
AWS::AppConfig::ConfigurationProfile	是	是	是	是	是	是	没有	没有
AWS::AppConfig::DeploymentStrategy	是	是	是	是	是	是	是	是
AWS::AppConfig::Environment	是	是	是	是	是	是	没有	没有
AWS::AppConfig::Extension	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::AppConfig::ExtensionAssociation	是	是	是	是	是	是	是	是
AWS::AppConfig::HostedConfiguration版本	是	是	是	是	是	是	没有	没有
AWS::AppFlow::Flow	是	是	是	是	没有	没有	没有	没有
AWS::AppIntegrations::Application	没有	是	是	没有	没有	没有	没有	没有
AWS::AppIntegrations::DataIntegration	没有	是	是	没有	没有	没有	没有	没有
AWS::AppIntegrations::EventIntegration	没有	是	是	没有	没有	没有	没有	没有
AWS::AppMesh::GatewayRoute	是	是	是	是	是	是	没有	没有
AWS::AppMesh::Mesh	是	是	是	是	是	是	没有	没有
AWS::AppMesh::Route	是	是	是	是	是	是	没有	没有
AWS::AppMesh::VirtualGateway	是	是	是	是	是	是	没有	没有
AWS::AppMesh::VirtualNode	是	是	是	是	是	是	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::AppMesh::VirtualRouter	是	是	是	是	是	是	没有	没有
AWS::AppMesh::VirtualService	是	是	是	是	是	是	没有	没有
AWS::AppRunner::Service	是	是	是	是	没有	没有	没有	没有
AWS::AppRunner::VpcConnector	是	是	没有	是	没有	没有	没有	没有
AWS::AppStream::AppBlock生成器	是	是	是	是	没有	没有	没有	没有
AWS::AppStream::Application	是	是	是	是	没有	没有	没有	没有
AWS::AppStream::DirectoryConfig	是	是	是	是	没有	没有	没有	没有
AWS::AppStream::Fleet	是	是	是	没有	没有	没有	没有	没有
AWS::AppStream::Stack	是	是	是	没有	没有	没有	没有	没有
AWS::AppSync::Api	是	是	是	是	是	是	是	是
AWS::AppSync::ApiCache	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::AppSync::GraphQLApi	是	是	是	是	是	是	是	是
AWS::Athena::DataCatalog	是	是	是	是	是	是	是	是
AWS::Athena::PreparedStatement	是	是	是	是	是	没有	是	是
AWS::Athena::WorkGroup	是	是	是	是	是	是	是	是
AWS::AuditManager::Assessment	是	是	是	没有	没有	没有	没有	没有
AWS::AutoScaling::AutoScaling群组	是	是	是	是	是	是	是	是
AWS::AutoScaling::LaunchConfiguration	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScalingPolicy	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScheduledAction	是	是	是	是	是	是	是	是
AWS::AutoScaling::WarmPool	是	是	是	是	是	是	没有	没有
AWS::BCMDataExports::Export	没有	没有	是	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Backup::BackupPlan	是	是	是	是	是	是	是	是
AWS::Backup::BackupSelection	是	是	是	是	是	是	是	是
AWS::Backup::BackupVault	是	是	是	是	是	是	是	是
AWS::Backup::RecoveryPoint	是	是	是	是	是	是	是	是
AWS::Backup::ReportPlan	是	是	是	是	是	是	没有	没有
AWS::Backup::RestoreTesting计划	是	是	是	是	是	是	是	是
AWS::BackupGateway::Hypervisor	是	是	是	是	是	是	没有	没有
AWS::Batch::ComputeEnvironment	是	是	是	是	是	是	是	是
AWS::Batch::JobQueue	是	是	是	是	是	是	是	是
AWS::Batch::SchedulingPolicy	是	是	是	是	是	是	是	是
AWS::Bedrock::ApplicationInference 配置文件	是	是	是	是	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Bedrock::Guardrail	是	是	是	是	是	是	是	是
AWS::Bedrock::KnowledgeBase	是	是	是	是	是	没有	没有	是
AWS::Bedrock::Prompt	是	是	是	是	是	是	是	是
AWS::BedrockAgentCore::BrowserCustom	是	是	没有	没有	没有	没有	没有	没有
AWS::BedrockAgentCore::CodeInterpreter自定义	是	是	没有	没有	没有	没有	没有	没有
AWS::BedrockAgentCore::Runtime	是	是	没有	没有	没有	没有	没有	没有
AWS::Cassandra::Keyspace	是	是	是	是	是	没有	没有	没有
AWS::CleanRoomsML::TrainingDataset	是	是	是	没有	是	没有	没有	没有
AWS::Cloud9::EnvironmentEC2	是	是	是	是	是	是	没有	没有
AWS::CloudFormation::GuardHook	是	是	是	是	是	是	是	是
AWS::CloudFormation::LambdaHook	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::CloudFormation::Stack	是	是	是	是	是	是	没有	是
AWS::CloudFormation::StackSet	是	是	是	是	是	是	是	是
AWS::CloudTrail::EventData存储	是	是	是	是	是	是	是	是
AWS::CloudTrail::Trail	是	是	是	是	是	是	是	是
AWS::CloudWatch::Alarm	是	是	是	是	是	是	是	是
AWS::CloudWatch::MetricStream	是	是	是	是	是	是	是	是
AWS::CodeArtifact::Domain	是	是	是	是	是	是	没有	没有
AWS::CodeArtifact::Repository	是	是	是	是	是	是	没有	没有
AWS::CodeBuild::Project	是	是	是	是	是	是	是	是
AWS::CodeBuild::ReportGroup	是	是	是	是	是	是	是	是
AWS::CodeDeploy::Application	是	是	是	是	是	是	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::CodeDeploy::DeploymentConfig	是	是	是	是	是	是	没有	没有
AWS::CodeDeploy::DeploymentGroup	是	是	是	是	是	是	没有	没有
AWS::CodeGuruProfiler::ProfilingGroup	是	是	是	没有	是	没有	没有	没有
AWS::CodeGuruReviewer::RepositoryAssociation	是	是	是	没有	是	没有	没有	没有
AWS::CodePipeline::Pipeline	是	是	是	是	是	是	是	是
AWS::Cognito::IdentityPool	是	是	是	是	是	是	是	是
AWS::Cognito::UserPool	是	是	是	是	是	是	是	是
AWS::Cognito::UserPool客户端	是	是	是	是	是	是	是	是
AWS::Cognito::UserPool群组	是	是	是	是	是	是	是	是
AWS::Comprehend::Flywheel	是	是	是	没有	没有	没有	没有	没有
AWS::Config::AggregationAuthorization	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Config::ConfigurationRecorder	是	是	是	是	是	是	是	是
AWS::Config::ConformancePack	是	是	是	是	是	是	是	是
AWS::Config::ConformancePack Compliance	是	是	是	是	是	是	是	是
AWS::Config::ResourceCompliance	是	是	是	是	是	是	是	是
AWS::Config::StoredQuery	是	是	是	是	是	是	是	是
AWS::Connect::Instance	没有	是	是	没有	没有	没有	没有	没有
AWS::Connect::PhoneNumber	没有	是	是	没有	没有	没有	没有	没有
AWS::Connect::QuickConnect	没有	是	是	没有	没有	没有	没有	没有
AWS::Connect::Rule	没有	是	是	没有	没有	没有	没有	没有
AWS::Connect::SecurityProfile	没有	是	是	没有	没有	没有	没有	没有
AWS::Connect::User	没有	是	是	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::CustomerProfiles::Domain	没有	是	是	没有	没有	没有	没有	没有
AWS::CustomerProfiles::ObjectType	没有	是	是	没有	没有	没有	没有	没有
AWS::DMS::Certificate	是	是	是	是	是	是	没有	没有
AWS::DMS::Endpoint	是	是	是	是	是	是	没有	没有
AWS::DMS::EventSubscription	是	是	是	是	是	是	没有	没有
AWS::DMS::MigrationProject	是	是	是	是	是	是	是	是
AWS::DMS::ReplicationInstance	是	是	是	是	是	是	没有	没有
AWS::DMS::ReplicationSubnet群组	是	是	是	是	是	是	没有	没有
AWS::DMS::ReplicationTask	是	是	是	是	是	是	没有	没有
AWS::DataSync::Agent	是	是	是	是	是	是	是	是
AWS::DataSync::LocationEFS	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::DataSync::LocationFSxLustre	是	是	是	是	是	是	没有	没有
AWS::DataSync::LocationFSx窗户	是	是	是	是	是	是	没有	没有
AWS::DataSync::LocationHDFS	是	是	是	是	是	是	是	是
AWS::DataSync::LocationNFS	是	是	是	是	是	是	是	是
AWS::DataSync::LocationObject存储	是	是	是	是	是	是	是	是
AWS::DataSync::LocationS3	是	是	是	是	是	是	是	是
AWS::DataSync::Location中小型企业	是	是	是	是	是	是	是	是
AWS::DataSync::Task	是	是	是	是	是	是	是	是
AWS::Deadline::Fleet	是	是	没有	没有	没有	没有	没有	没有
AWS::Deadline::Monitor	是	是	没有	没有	没有	没有	没有	没有
AWS::Deadline::QueueFleet协会	是	是	没有	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Detective::Graph	是	是	是	是	是	是	没有	没有
AWS::DynamoDB::Table	是	是	是	是	是	是	是	是
AWS::EC2::Capacity Reservation	是	是	是	是	是	是	是	是
AWS::EC2::CarrierGateway	是	是	是	是	没有	没有	没有	没有
AWS::EC2::ClientVpn端点	是	是	是	是	是	是	没有	是
AWS::EC2::ClientVpnTargetNetworkAssociation	是	是	是	是	是	是	没有	是
AWS::EC2::CustomerGateway	是	是	是	是	是	是	是	是
AWS:EC2::: DHCPOptions	是	是	是	是	是	是	是	是
AWS:EC2:: EC2 舰队	是	是	是	是	是	是	是	是
AWS:::EC2: EIP	是	是	是	是	是	是	是	是
AWS:EC2::: EIPAssociation	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::EgressOnlyInternetGateway	是	是	是	是	是	是	没有	是
AWS::EC2::FlowLog	是	是	是	是	是	是	是	是
AWS::EC2::Host	是	是	是	是	是	是	是	是
AWS:::EC2: IPAM	是	是	是	是	是	是	是	是
AWS:EC2::: IPAMPool	是	是	是	是	是	是	是	是
AWS::EC2:: IPAMPool Cidr	是	是	是	是	是	是	是	是
AWS::EC2: IPAMResource Discovery	是	是	是	是	是	是	是	是
AWS:EC2::: IPAMResource DiscoveryAssociation	是	是	是	是	是	是	是	是
AWS:EC2::: IPAMScope	是	是	是	是	是	是	是	是
AWS::EC2::Instance	是	是	是	是	是	是	是	是
AWS::EC2::InstanceConnect端点	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::InternetGateway	是	是	是	是	是	是	是	是
AWS::EC2::LaunchTemplate	是	是	是	是	是	是	没有	没有
AWS::EC2::NatGateway	是	是	是	是	是	是	没有	是
AWS::EC2::NetworkAcl	是	是	是	是	是	是	是	是
AWS::EC2::NetworkInsightsAccessScope	是	是	是	是	是	是	没有	没有
AWS::EC2::NetworkInsightsAccessScopeAnalysis	是	是	是	是	是	是	没有	没有
AWS::EC2::NetworkInsights分析	是	是	是	是	是	是	没有	没有
AWS::EC2::NetworkInsights路径	是	是	是	是	是	是	没有	没有
AWS::EC2::NetworkInterface	是	是	是	是	是	是	是	是
AWS::EC2::PrefixList	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::RouteTable	是	是	是	是	是	是	是	是
AWS::EC2::SecurityGroup	是	是	是	是	是	是	是	是
AWS::EC2::SecurityGroupVpcAssociation	是	是	是	是	是	是	是	是
AWS::EC2::SnapshotBlockPublicAccess	是	是	是	是	是	是	是	是
AWS::EC2::SpotFleet	是	是	是	是	是	是	是	是
AWS::EC2::Subnet	是	是	是	是	是	是	是	是
AWS::EC2::SubnetCidr屏蔽	是	是	是	是	是	是	是	是
AWS::EC2::SubnetNetworkAclAssociation	是	是	是	是	是	是	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是	是	是	是	是	是	是
AWS::EC2::TrafficMirror过滤器	是	是	是	是	是	是	是	是
AWS::EC2::TrafficMirrorSession	是	是	是	是	是	没有	没有	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::TrafficMirror目标	是	是	是	是	是	是	没有	是
AWS::EC2::TransitGateway	是	是	是	是	是	是	是	是
AWS::EC2::TransitGateway附件	是	是	是	是	是	是	是	是
AWS::EC2::TransitGatewayConnect	是	是	是	是	是	是	没有	是
AWS::EC2::TransitGatewayMulticastDomain	是	是	是	是	是	是	是	是
AWS::EC2::TransitGatewayRouteTable	是	是	是	是	是	是	没有	是
AWS:::EC2: VPC	是	是	是	是	是	是	是	是
AWS:EC2::: VPCBlockPublicAccessExclusion	是	是	是	是	是	是	是	是
AWS:EC2::: VPCBlockPublicAccessOptions	是	是	是	是	是	是	是	是
AWS:EC2::: VPCEndpoint	是	是	是	是	是	是	是	是
AWS:EC2::: VPCEndpoint ConnectionNotification	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS:EC2::: VPCEndpoint 服务	是	是	是	是	是	是	是	是
AWS::EC2:: VPCGateway 附件	是	是	是	是	是	是	是	是
AWS:EC2:: VPCPeering 连接	是	是	是	是	是	是	是	是
AWS:EC2::: VPNConnection	是	是	是	是	是	是	是	是
AWS::EC2:: VPNConnection 路线	是	是	是	是	是	是	是	是
AWS:EC2::: VPNGateway	是	是	是	是	是	是	是	是
AWS::EC2::VerifiedAccess实例	是	是	是	没有	是	是	没有	没有
AWS::EC2::Volume	是	是	是	是	是	是	是	是
AWS::ECR::PullThroughCacheRule	是	是	是	是	是	是	是	是
AWS::ECR::RegistryPolicy	是	是	是	是	是	是	是	是
AWS::ECR::ReplicationConfiguration	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ECR::Repository	是	是	是	是	是	是	是	是
AWS::ECR::RepositoryCreation模板	是	是	是	是	是	是	是	是
AWS::ECS::CapacityProvider	是	是	是	是	是	是	是	是
AWS::ECS::Cluster	是	是	是	是	是	是	是	是
AWS::ECS::Service	是	是	是	是	是	是	是	是
AWS::ECS::TaskDefinition	是	是	是	是	是	是	是	是
AWS::ECS::TaskSet	是	是	是	是	是	是	是	是
AWS::EFS::AccessPoint	是	是	是	是	是	是	是	是
AWS::EFS::FileSystem	是	是	是	是	是	是	是	是
AWS::EKS::Addon	是	是	是	是	是	是	是	是
AWS::EKS::Cluster	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EKS::FargateProfile	是	是	是	是	是	是	是	是
AWS::EKS::IdentityProviderConfig	是	是	是	是	是	是	是	是
AWS::EMR::SecurityConfiguration	是	是	是	是	是	是	是	是
AWS::EMR::Studio	是	是	是	是	是	是	是	是
AWS::EMRContainers::VirtualCluster	是	是	是	是	是	是	是	是
AWS::EMRServerless::Application	是	是	是	是	是	是	没有	没有
AWS::ElasticBeanstalk::Application	是	是	是	是	是	是	是	是
AWS::ElasticBeanstalk::ApplicationVersion	是	是	是	是	是	是	是	是
AWS::ElasticBeanstalk::Environment	是	是	是	是	是	是	是	是
AWS::ElasticLoadBalancing::LoadBalancer	是	是	是	是	是	是	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是	是	是	是	是	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是	是	是	是	是	是	是
AWS::ElasticLoadBalancingV2::TargetGroup	是	是	是	是	是	是	是	是
AWS::Elasticsearch::Domain	是	是	是	是	是	是	是	是
AWS::EntityResolution::IdMapping工作流程	是	是	是	没有	没有	没有	没有	没有
AWS::EntityResolution::MatchingWorkflow	是	是	是	没有	没有	没有	没有	没有
AWS::EntityResolution::SchemaMapping	是	是	是	没有	没有	没有	没有	没有
AWS::EventSchemas::Discoverer	是	是	是	是	是	是	是	是
AWS::EventSchemas::Registry	是	是	是	是	是	是	是	是
AWS::EventSchemas::RegistryPolicy	是	是	是	是	是	是	是	是
AWS::EventSchemas::Schema	是	是	是	是	是	是	是	是
AWS::Events::ApiDestination	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Events::Archive	是	是	是	是	是	是	是	是
AWS::Events::Connection	是	是	是	是	是	是	是	是
AWS::Events::Endpoint	是	是	是	是	是	没有	没有	没有
AWS::Events::EventBus	是	是	是	是	是	是	是	是
AWS::Events::Rule	是	是	是	是	是	是	是	是
AWS::FIS::ExperimentTemplate	是	是	是	是	是	是	是	没有
AWS::Forecast::Dataset	是	是	没有	没有	没有	没有	没有	没有
AWS::Forecast::DatasetGroup	是	是	没有	没有	没有	没有	没有	没有
AWS::FraudDetector::EntityType	是	没有	没有	没有	没有	没有	没有	没有
AWS::FraudDetector::Label	是	没有	没有	没有	没有	没有	没有	没有
AWS::FraudDetector::Outcome	是	没有	没有	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::FraudDetector::Variable	是	没有	没有	没有	没有	没有	没有	没有
AWS::GameLift::Alias	是	是	是	没有	没有	没有	没有	没有
AWS::GameLift::Build	是	是	是	没有	没有	没有	没有	没有
AWS::GameLift::GameSession队列	是	是	是	没有	没有	没有	没有	没有
AWS::GameLift::MatchmakingConfiguration	是	是	没有	没有	没有	没有	没有	没有
AWS::Glue::Classifier	是	是	是	是	是	是	是	是
AWS::Glue::Database	是	是	是	是	是	没有	没有	没有
AWS::Glue::Job	是	是	是	是	是	是	是	是
AWS::Glue::MLTransform	是	是	是	是	是	是	是	是
AWS::Glue::Registry	是	是	是	是	是	是	没有	没有
AWS::Grafana::Workspace	是	是	是	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::GreengrassV2::ComponentVersion	是	是	是	没有	没有	没有	没有	没有
AWS::GroundStation::Config	是	是	没有	没有	是	没有	没有	没有
AWS::GroundStation::DataflowEndpoint群组	是	是	没有	没有	是	没有	没有	没有
AWS::GroundStation::MissionProfile	是	是	没有	没有	是	没有	没有	没有
AWS::GuardDuty::Detector	是	是	是	是	是	是	是	是
AWS::GuardDuty::Filter	是	是	是	是	是	是	没有	没有
AWS::Guard职责:: IPSet	是	是	是	是	是	是	没有	没有
AWS::GuardDuty::MalwareProtection计划	是	是	是	是	是	是	是	是
AWS::GuardDuty::ThreatIntelSet	是	是	是	是	是	是	是	是
AWS::Health湖::FHIRDatastore	是	没有	是	没有	没有	没有	没有	没有
AWS::IAM::Group	是	是	是	是	是	是	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IAM::Policy	是	是	是	是	是	是	没有	没有
AWS::IAM::Role	是	是	是	是	是	是	没有	没有
AWS::IAM::User	是	是	是	是	是	是	没有	没有
AWS::IVS::Channel	是	是	没有	没有	没有	没有	没有	没有
AWS::IVS::PlaybackKey配对	是	是	没有	没有	没有	没有	没有	没有
AWS::IVS::RecordingConfiguration	是	是	没有	没有	没有	没有	没有	没有
AWS::ImageBuilder::ContainerRecipe	是	是	是	是	是	是	是	是
AWS::ImageBuilder::DistributionConfiguration	是	是	是	是	是	是	是	是
AWS::ImageBuilder::ImagePipeline	是	是	是	是	是	是	是	是
AWS::ImageBuilder::ImageRecipe	是	是	是	是	是	是	是	是
AWS::ImageBuilder::InfrastructureConfiguration	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ImageBuilder::LifecyclePolicy	是	是	是	是	是	是	是	是
AWS::InspectorV2::Activation	是	是	是	是	是	是	是	是
AWS::InspectorV2::Filter	是	是	是	是	是	是	没有	是
AWS::IoT::AccountAudit配置	是	是	是	是	是	没有	没有	没有
AWS::IoT::Authorizer	是	是	是	是	是	没有	没有	没有
AWS::IoT:: CACertificate	是	是	是	是	是	没有	没有	没有
AWS::IoT::CustomMetric	是	是	是	是	是	没有	没有	没有
AWS::IoT::Dimension	是	是	是	是	是	没有	没有	没有
AWS::IoT::DomainConfiguration	是	是	是	是	是	没有	没有	没有
AWS::IoT::FleetMetric	是	是	是	是	是	没有	没有	没有
AWS::IoT::JobTemplate	是	是	是	是	是	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IoT::MitigationAction	是	是	是	是	是	没有	没有	没有
AWS::IoT::Policy	是	是	是	是	是	没有	没有	没有
AWS::IoT::ProvisioningTemplate	是	是	是	是	是	没有	没有	没有
AWS::IoT::RoleAlias	是	是	是	是	是	没有	没有	没有
AWS::IoT::ScheduledAudit	是	是	是	是	是	没有	没有	没有
AWS::IoT::SecurityProfile	是	是	是	是	是	没有	没有	没有
AWS::IoT::ThingGroup	是	是	是	是	是	没有	是	没有
AWS::IoTAnalytics::Channel	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTAnalytics::Dataset	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTAnalytics::Datastore	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTAnalytics::Pipeline	是	是	没有	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IoTCoreDeviceAdvisor::SuiteDefinition	是	没有	没有	没有	没有	没有	没有	没有
AWS::IoTEvents::AlarmModel	是	是	是	没有	没有	没有	没有	没有
AWS::IoTEvents::DetectorModel	是	是	是	没有	没有	没有	没有	没有
AWS::IoTEvents::Input	是	是	是	没有	没有	没有	没有	没有
AWS::IoTSiteWise::Asset	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTSiteWise::AssetModel	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTSiteWise::Dashboard	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTSiteWise::Gateway	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTSiteWise::Portal	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTSiteWise::Project	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTTwinMaker::ComponentType	是	是	没有	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IoTTwinMaker::Entity	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTTwinMaker::Scene	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTTwinMaker::SyncJob	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTTwinMaker::Workspace	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTWireless::FuotaTask	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTWireless::MulticastGroup	是	是	没有	没有	没有	没有	没有	没有
AWS::IoTWireless::ServiceProfile	是	是	没有	没有	没有	没有	没有	没有
AWS::KMS::Alias	是	是	是	是	是	是	没有	是
AWS::KMS::Key	是	是	是	是	是	是	是	是
AWS::KafkaConnect::Connector	是	是	是	是	是	没有	没有	没有
AWS::KafkaConnect::CustomPlugin	是	是	是	是	是	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Kendra::Index	是	没有	是	没有	没有	没有	没有	没有
AWS::Kinesis::Stream	是	是	是	是	是	是	是	是
AWS::Kinesis::StreamConsumer	是	是	是	是	是	是	是	是
AWS::KinesisAnalyticsV2::Application	是	是	是	是	是	是	是	是
AWS::KinesisFirehose::DeliveryStream	是	是	是	是	是	是	是	是
AWS::KinesisVideo::SignalingChannel	是	是	是	是	没有	没有	没有	没有
AWS::KinesisVideo::Stream	是	是	是	是	没有	没有	没有	没有
AWS::Lambda::CodeSigningConfig	是	是	是	是	是	是	没有	没有
AWS::Lambda::Function	是	是	是	是	是	是	是	是
AWS::Lex::Bot	是	是	是	没有	没有	没有	没有	没有
AWS::Lex::BotAlias	是	是	是	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Lightsail::Bucket	是	是	是	是	是	没有	没有	没有
AWS::Lightsail::Certificate	是	是	是	是	是	没有	没有	没有
AWS::Lightsail::Disk	是	是	是	是	是	没有	没有	没有
AWS::Lightsail::StaticIp	是	是	是	是	是	没有	没有	没有
AWS::Location::APIKey	是	是	是	没有	是	没有	没有	没有
AWS::Location::GeofenceCollection	是	是	是	没有	是	没有	是	没有
AWS::Location::Map	是	是	是	没有	是	没有	是	没有
AWS::Location::PlaceIndex	是	是	是	没有	是	没有	是	没有
AWS::Location::RouteCalculator	是	是	是	没有	是	没有	是	没有
AWS::Logs::Destination	是	是	是	是	是	是	是	是
AWS::LookoutVision::Project	是	是	没有	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::M2::Environment	是	是	是	是	是	是	没有	没有
AWS::MSK::BatchScram秘密	是	是	是	是	是	是	是	是
AWS::MSK::Cluster	是	是	是	是	是	是	是	是
AWS::MSK::ClusterPolicy	是	是	是	是	是	是	是	是
AWS::MSK::Configuration	是	是	是	是	是	是	是	是
AWS::MSK::ServerlessCluster	是	是	是	是	是	没有	没有	没有
AWS::MSK::VpcConnection	是	是	是	是	是	是	是	是
AWS::Macie::Session	是	是	是	是	是	是	没有	没有
AWS::MediaConnect::FlowEntitlement	是	是	是	是	是	没有	没有	没有
AWS::MediaConnect::FlowSource	是	是	是	是	是	没有	没有	没有
AWS::MediaConnect::FlowVpc接口	是	是	是	是	是	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::MediaConnect::Gateway	是	是	是	是	是	没有	没有	没有
AWS::MediaLive::Multiplexprogram	是	是	是	是	是	没有	没有	没有
AWS::MediaPackage::Asset	是	是	是	是	是	没有	没有	没有
AWS::MediaPackage::PackagingConfiguration	是	是	是	是	是	没有	没有	没有
AWS::MediaPackage::PackagingGroup	是	是	是	是	是	没有	没有	没有
AWS::MediaPackageV2::Channel	是	是	是	是	是	没有	没有	没有
AWS::MediaPackageV2::ChannelGroup	是	是	是	是	是	没有	没有	没有
AWS::MediaPackageV2::OriginEndpoint	是	是	是	是	是	没有	没有	没有
AWS::MediaTailor::LiveSource	是	是	没有	是	是	没有	没有	没有
AWS::MediaTailor::PlaybackConfiguration	是	是	没有	是	是	没有	没有	没有
AWS::MemoryDB::SubnetGroup	是	是	是	是	是	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::NetworkFirewall::Firewall	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::RuleGroup	是	是	是	是	是	是	是	是
AWS::Network防火墙:: TLSInspection 配置	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::VpcEndpoint协会	是	是	是	是	是	是	是	是
AWS::Omics::RunGroup	是	是	是	没有	没有	没有	没有	没有
AWS::Omics::Workflow	是	是	是	没有	没有	没有	没有	没有
AWS::OpenSearch::Domain	是	是	是	是	是	是	没有	没有
AWS::OpenSearchServerless::Collection	是	是	是	是	是	没有	没有	没有
AWS::OpenSearchServerless::SecurityConfig	是	是	是	是	是	是	是	是
AWS::OpenSearchServerless::VpcEndpoint	是	是	是	是	是	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::PCAConnectorAD::Connector	是	是	是	是	是	是	是	是
AWS::PCAConnectorAD::DirectoryRegistration	是	是	是	是	是	是	是	是
AWS::Panorama::Package	是	没有	没有	没有	没有	没有	没有	没有
AWS::Personalize::Dataset	是	是	没有	没有	没有	没有	没有	没有
AWS::Personalize::DatasetGroup	是	是	没有	没有	没有	没有	没有	没有
AWS::Personalize::Schema	是	是	没有	没有	没有	没有	没有	没有
AWS::Personalize::Solution	是	是	没有	没有	没有	没有	没有	没有
AWS::Pinpoint::App	是	是	是	没有	没有	没有	没有	没有
AWS::Pinpoint::ApplicationSettings	是	是	是	没有	没有	没有	没有	没有
AWS::Pinpoint::Campaign	是	是	是	没有	没有	没有	没有	没有
AWS::Pinpoint::EmailChannel	是	是	是	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Pinpoint::EmailTemplate	是	是	是	没有	没有	没有	没有	没有
AWS::Pinpoint::EventStream	是	是	是	没有	没有	没有	没有	没有
AWS::Pinpoint::InApp模板	是	是	是	没有	没有	没有	没有	没有
AWS::Pinpoint::Segment	是	是	是	没有	没有	没有	没有	没有
AWS::QuickSight::Dashboard	是	是	是	是	是	是	没有	是
AWS::QuickSight::DataSource	是	是	是	是	是	没有	没有	没有
AWS::QuickSight::Template	是	是	是	是	是	没有	没有	没有
AWS::QuickSight::Theme	是	是	是	是	是	没有	没有	没有
AWS:: RDS:: DBCluster	是	是	是	是	是	是	是	是
AWS:: RDS:: 快照 DBCluster	是	是	是	是	是	是	是	是
AWS:: RDS:: DBInstance	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS:: RDS:: 终端节点 DBProxy	是	是	是	是	是	是	是	是
AWS:: RDS:: 群组 DBSecurity	是	是	是	是	是	是	是	是
AWS:: RDS:: DBSnapshot	是	是	是	是	是	是	是	是
AWS:: RDS:: 群组 DBSubnet	是	是	是	是	是	是	是	是
AWS::RDS::EventSubscription	是	是	是	是	是	是	是	是
AWS::RDS::GlobalCluster	是	是	是	是	是	是	是	是
AWS::RDS::Integration	是	是	是	是	是	是	是	是
AWS::RDS::OptionGroup	是	是	是	是	是	是	是	是
AWS::RUM::AppMonitor	是	是	是	是	是	是	是	是
AWS::Redshift::Cluster	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterParameter群组	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Redshift::ClusterSecurity群组	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSnapshot	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSubnet群组	是	是	是	是	是	是	是	是
AWS::Redshift::EndpointAccess	是	是	是	是	是	没有	没有	没有
AWS::Redshift::EndpointAuthorization	是	是	是	是	是	没有	没有	没有
AWS::Redshift::EventSubscription	是	是	是	是	是	是	是	是
AWS::Redshift::Integration	是	是	是	是	是	是	是	是
AWS::Redshift::ScheduledAction	是	是	是	是	是	是	没有	没有
AWS::ResilienceHub::App	是	是	是	是	是	是	没有	没有
AWS::ResilienceHub::ResiliencyPolicy	是	是	是	是	是	是	没有	没有
AWS::ResourceExplorer2::Index	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::RoboMaker::RobotApplication	是	是	没有	没有	没有	没有	没有	没有
AWS::RoboMaker::RobotApplication版本	是	是	没有	没有	没有	没有	没有	没有
AWS::RoboMaker::SimulationApplication	是	是	没有	没有	没有	没有	没有	没有
AWS::Roles任何地方:: CRL	是	是	是	是	是	是	是	是
AWS::RolesAnywhere::Profile	是	是	是	是	是	是	是	是
AWS::RolesAnywhere::TrustAnchor	是	是	是	是	是	是	是	是
AWS::Route53Profiles::Profile	是	是	是	是	是	是	是	是
AWS::Route53Profiles::ProfileAssociation	是	是	是	是	是	是	是	是
AWS::Route53Resolver::FirewallDomain名单	是	是	是	是	是	是	没有	没有
AWS::Route53Resolver::FirewallRule群组	是	是	是	是	是	是	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverEndpoint	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是	是	是	是	是	是	没有
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	是	是	是	是	是	是	是	没有
AWS::Route53Resolver::ResolverRule	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverRule协会	是	是	是	是	是	是	是	是
AWS::S3::AccessGrant	是	是	是	是	是	是	是	是
AWS::S3::AccessGrants实例	是	是	是	是	是	是	是	是
AWS::S3::AccessGrantsLocation	是	是	是	是	是	是	是	是
AWS::S3::AccessPoint	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::S3::AccountPublicAccessBlock	是	是	是	是	是	是	是	是
AWS::S3::Bucket	是	是	是	是	是	是	是	是
AWS::S3::StorageLens	是	是	是	是	是	没有	没有	没有
AWS::S3::StorageLens群组	是	是	是	是	是	没有	没有	没有
AWS::S3Express::BucketPolicy	是	没有	没有	没有	是	没有	没有	没有
AWS::S3Express::DirectoryBucket	是	没有	没有	没有	是	没有	没有	没有
AWS::S3Tables::TableBucket	是	是	是	是	是	是	是	是
AWS::S3Tables::TableBucket政策	是	是	是	是	是	是	是	是
AWS::SES::ConfigurationSet	是	是	是	是	是	是	没有	没有
AWS::SES::ContactList	是	是	是	是	是	是	没有	没有
AWS::SES::DedicatedIp泳池	是	是	是	是	是	是	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::SES::MailManagerTrafficPolicy	是	是	是	是	是	没有	没有	没有
AWS::SES::ReceiptFilter	是	是	是	是	是	没有	没有	没有
AWS::SES::ReceiptRuleSet	是	是	是	是	是	没有	没有	没有
AWS::SES::Template	是	是	是	是	是	是	没有	没有
AWS::SNS::Topic	是	是	是	是	是	是	是	是
AWS::SQS::Queue	是	是	是	是	是	是	没有	没有
AWS::SSM::AssociationCompliance	是	是	是	是	是	是	是	是
AWS::SSM::Document	是	是	是	是	是	是	是	是
AWS::SSM::FileData	是	是	是	是	是	是	是	是
AWS::SSM::ManagedInstance 清单	是	是	是	是	是	是	是	是
AWS::SSM::PatchCompliance	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::SSM::ResourceData同步	是	是	是	是	是	是	是	是
AWS::SSMContacts::Contact	是	是	是	是	是	没有	没有	没有
AWS::SSMIncidents::ResponsePlan	是	是	是	是	是	没有	没有	没有
AWS::SageMaker::AppImageConfig	是	是	是	是	是	是	是	没有
AWS::SageMaker::CodeRepository	是	是	是	是	是	是	没有	没有
AWS::SageMaker::DataQualityJobDefinition	是	是	是	是	是	没有	没有	没有
AWS::SageMaker::Domain	是	是	是	是	是	是	没有	没有
AWS::SageMaker::EndpointConfig	是	是	是	是	是	是	没有	没有
AWS::SageMaker::FeatureGroup	是	是	是	是	是	是	是	没有
AWS::SageMaker::Image	是	是	是	是	是	是	是	没有
AWS::SageMaker::InferenceExperiment	是	是	是	是	是	是	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::SageMaker::MlflowTracking服务器	是	是	是	是	是	是	是	是
AWS::SageMaker::Model	是	是	是	是	是	是	没有	没有
AWS::SageMaker::ModelBiasJobDefinition	是	是	是	是	是	没有	没有	没有
AWS::SageMaker::ModelExplainabilityJobDefinition	是	是	是	是	是	没有	没有	没有
AWS::SageMaker::ModelQualityJobDefinition	是	是	是	是	是	没有	没有	没有
AWS::SageMaker::MonitoringSchedule	是	是	是	是	是	没有	没有	没有
AWS::SageMaker::NotebookInstance	是	是	是	是	是	是	没有	没有
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	是	是	是	是	是	没有	没有
AWS::SageMaker::StudioLifecycleConfig	是	是	是	是	是	是	是	是
AWS::SageMaker::UserProfile	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::SageMaker::Workteam	是	是	是	没有	没有	没有	没有	没有
AWS::SecretsManager::ResourcePolicy	是	是	是	是	是	是	是	是
AWS::SecretsManager::RotationSchedule	是	是	是	是	是	是	是	是
AWS::SecretsManager::Secret	是	是	是	是	是	是	是	是
AWS::SecurityHub::Standard	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::CloudFormation产品	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::Portfolio	是	是	是	是	是	是	是	是
AWS::ServiceDiscovery::HttpNamespace	是	是	是	是	是	是	是	是
AWS::ServiceDiscovery::Instance	是	是	是	是	是	是	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ServiceDiscovery::PublicDns命名空间	是	是	是	是	是	是	是	是
AWS::ServiceDiscovery::Service	是	是	是	是	是	是	没有	没有
AWS::ShieldRegional::Protection	是	是	是	是	是	是	是	是
AWS::Signer::SigningProfile	是	是	是	是	是	是	没有	没有
AWS::StepFunctions::Activity	是	是	是	是	是	是	是	是
AWS::StepFunctions::StateMachine	是	是	是	是	是	是	是	是
AWS::Transfer::Agreement	是	是	是	是	是	是	没有	没有
AWS::Transfer::Certificate	是	是	是	是	是	是	是	是
AWS::Transfer::Connector	是	是	是	是	是	是	是	是
AWS::Transfer::Profile	是	是	是	是	是	是	是	是
AWS::Transfer::Server	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Transfer::Workflow	是	是	是	是	是	是	是	是
AWS::WAFRegional::RateBased规则	是	是	是	是	是	是	是	是
AWS::WAFRegional::Rule	是	是	是	是	是	是	是	是
AWS::WAFRegional::RuleGroup	是	是	是	是	是	是	是	是
AWS::WAFRegional::WebACL	是	是	是	是	是	是	是	是
AWS:WAFv2::: IPSet	是	是	是	是	是	是	是	是
AWS::WAFv2::ManagedRuleSet	是	是	是	是	是	是	是	是
AWS::WAFv2::RegexPatternSet	是	是	是	是	是	是	是	是
AWS::WAFv2::RuleGroup	是	是	是	是	是	是	是	是
AWS::WAFv2::WebACL	是	是	是	是	是	是	是	是
AWS::WorkSpaces::ConnectionAlias	是	是	是	没有	没有	没有	没有	没有

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::WorkSpaces::Workspace	是	是	是	没有	没有	没有	没有	没有
AWS::XRay::EncryptionConfig	是	是	是	是	是	是	是	是

亚太区域

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::ACM::Certificate	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::ACMPCA::CertificateAuthority激活	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::APS::RuleGroups命名空间	是	是	是	是	没有	是	是	是	是	是	没有	是	是
AWS::AccessAnalyzer::Analyzer	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::AmazonMQ::Broker	是	没有	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::Amplify::App	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Amplify::Branch	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::ApiGateway::DomainName	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ApiGateway::Method	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ApiGateway::RestApi	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ApiGateway::Stage	是	是	是	是	是	是	是	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::ApiGateway::UsagePlan	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Api	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ApiGatewayV2::Integration	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ApiGatewayV2::Stage	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::AppConfig::Application	是	没有	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::AppConfig::ConfigurationProfile	是	没有	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::AppConfig::DeploymentStrategy	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::AppConfig::Environment	是	没有	是	没有	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::AppConfig::Extension	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::AppConfig::ExtensionAssociation	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::AppConfig::HostedConfiguration版本	是	没有	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::AppFlow::Flow	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::AppIntegrations::Application	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::AppIntegrations::DataIntegration	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::AppIntegrations::EventIntegration	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::AppMesh::GatewayRoute	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::AppMesh::Mesh	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::AppMesh::Route	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::AppMesh::VirtualGateway	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::AppMesh::VirtualNode	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::AppMesh::VirtualRouter	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::AppMesh::VirtualService	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::AppRunner::Service	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::AppRunner::VpcConnector	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是
AWS::AppStream::AppBlock生成器	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::AppStream::Application	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::AppStream::DirectoryConfig	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::AppStream::Fleet	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::AppStream::Stack	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::AppSync::Api	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::AppSync::ApiCache	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::AppSync::GraphQLApi	是	是	是	是	是	是	是	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Athena::DataCatalog	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Athena::PreparedStatement	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Athena::WorkGroup	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::AuditManager::Assessment	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是
AWS::AutoScaling::AutoScaling群组	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::AutoScaling::LaunchConfiguration	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScalingPolicy	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::AutoScaling::ScheduledAction	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::AutoScaling::WarmPool	是	是	是	是	没有	是	是	是	是	是	没有	没有	是
AWS::Backup::BackupPlan	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Backup::BackupSelection	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Backup::BackupVault	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Backup::RecoveryPoint	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::Backup::ReportPlan	是	是	是	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Backup::RestoreTesting计划	是	是	是	没有	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::BackupGateway::Hypervisor	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Batch::ComputeEnvironment	是	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Batch::JobQueue	是	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Batch::SchedulingPolicy	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Bedrock::ApplicationInference 配置文件	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Bedrock::Guardrail	没有	是	是	是	没有	是	是	是	是	是	没有	没有	是
AWS::Bedrock::KnowledgeBase	没有	是	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Bedrock::Prompt	没有	是	没有	没有	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::BedrockAgentCore::BrowserCustom	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是
AWS::BedrockAgentCore::CodeInterpreter自定义	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是
AWS::BedrockAgentCore::Runtime	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是
AWS::Cassandra::Keyspace	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::CleanRoomsML::TrainingDataset	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Cloud9::EnvironmentEC2	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::CloudFormation::GuardHook	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::CloudFormation::LambdaHook	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::CloudFormation::Stack	是	没有	是	是	没有	是	是	是	是	是	是	是	是
AWS::CloudFormation::StackSet	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::CloudTrail::EventData存储	是	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::CloudTrail::Trail	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::CloudWatch::Alarm	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::CloudWatch::MetricStream	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::CodeArtifact::Domain	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::CodeArtifact::Repository	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是
AWS::CodeBuild::Project	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::CodeBuild::ReportGroup	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::CodeDeploy::Application	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::CodeDeploy::DeploymentConfig	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::CodeDeploy::DeploymentGroup	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::CodeGuruProfiler::ProfilingGroup	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::CodeGuruReviewer::RepositoryAssociation	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	是
AWS::CodePipeline::Pipeline	是	是	没有	没有	是	是	没有	是	是	是	没有	没有	是
AWS::Cognito::IdentityPool	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Cognito::UserPool	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Cognito::UserPool客户端	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Cognito::UserPool群组	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Comprehend::Flywheel	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Config::AggregationAuthorization	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Config::ConfigurationRecorder	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Config::ConformancePack	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::Config::ConformancePackCompliance	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::Config::ResourceCompliance	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Config::StoredQuery	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Connect::Instance	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Connect::PhoneNumber	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Connect::QuickConnect	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Connect::Rule	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Connect::SecurityProfile	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Connect::User	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::CustomerProfiles::Domain	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::CustomerProfiles::ObjectType	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::DMS::Certificate	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::DMS::Endpoint	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::DMS::EventSubscription	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::DMS::MigrationProject	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::DMS::ReplicationInstance	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::DMS::ReplicationSubnet群组	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::DMS::ReplicationTask	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::DataSync::Agent	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::DataSync::LocationEFS	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::DataSync::LocationFSxLustre	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::DataSync::LocationFSx窗户	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::DataSync::LocationHDFS	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::DataSync::LocationNFS	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::DataSync::LocationObject存储	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::DataSync::LocationS3	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::DataSync::Location中小型企业	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::DataSync::Task	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Deadline::Fleet	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Deadline::Monitor	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	是
AWS::Deadline::QueueFleet协会	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Detective::Graph	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::DynamoDB::Table	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::CapacityReservation	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::EC2::CarrierGateway	没有	没有	没有	没有	没有	没有	没有	是	没有	是	没有	没有	是
AWS::EC2::ClientVpn端点	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EC2::ClientVpnTargetNetworkAssociation	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::EC2::CustomerGateway	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:EC2:::DHCPOptions	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS:EC2::EC2 舰队	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS:::EC2: EIP	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:EC2:::EIPAssociation	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EC2::EgressOnlyInternetGateway	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::EC2::FlowLog	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EC2::Host	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:::EC2: IPAM	是	是	是	没有	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS:EC2::: IPAMPool	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::EC2::IPAMPool Cidr	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::EC2:IPAMResource Discovery	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS:EC2:::IPAMResource Discovery Association	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS:EC2::: IPAMScope	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::EC2::Instance	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::Instance Connect端点	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EC2::InternetGateway	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::EC2::LaunchTemplate	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::EC2::NatGateway	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::EC2::NetworkAcl	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::NetworkInsightsAccessScope	是	是	是	是	没有	是	是	是	是	是	没有	是	是
AWS::EC2::NetworkInsightsAccessScopeAnalysis	是	是	是	是	没有	是	是	是	是	是	没有	是	是
AWS::EC2::NetworkInsights分析	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::EC2::NetworkInsights路径	是	是	是	是	没有	是	是	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::EC2::NetworkInterface	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::PrefixList	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EC2::RouteTable	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::SecurityGroup	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::SecurityGroupVpcAssociation	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::SnapshotBlockPublicAccess	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EC2::SpotFleet	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EC2::Subnet	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::EC2::SubnetCidr屏蔽	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::SubnetNetworkAclAssociation	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EC2::SubnetRouteTableAssociation	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EC2::TrafficMirror过滤器	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EC2::TrafficMirrorSession	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EC2::TrafficMirror目标	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EC2::TransitGateway	是	是	是	是	是	是	是	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::EC2::TransitGateway附件	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EC2::TransitGatewayConnect	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EC2::TransitGatewayMulticastDomain	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EC2::TransitGatewayRouteTable	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS:::EC2: VPC	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:EC2:: : VPCBlockPublicAccessExclusion	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS:EC2::: VPCBlockPublicAccessOptions	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS:EC2::: VPCEndpoint	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:EC2::: VPCEndpoint ConnectionNotification	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS:EC2::: VPCEndpoint 服务	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::VPCGateway 附件	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:EC2::VPCPeering 连接	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:EC2:::VPNConnection	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::EC2::VPNConnection 路线	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS:EC2:::VPNGateway	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EC2::Verified Access实例	没有	没有	是	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::EC2::Volume	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ECR::PullThroughCacheRule	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::ECR::RegistryPolicy	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::ECR::ReplicationConfiguration	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ECR::Repository	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::ECR::RepositoryCreationTemplate	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ECS::CapacityProvider	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::ECS::Cluster	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ECS::Service	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ECS::TaskDefinition	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ECS::TaskSet	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EFS::AccessPoint	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EFS::FileSystem	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::EKS::Addon	是	是	是	没有	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::EKS::Cluster	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EKS::FargateProfile	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EKS::IdentityProviderConfig	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::EMR::SecurityConfiguration	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::EMR::Studio	是	没有	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::EMRContainers::VirtualCluster	是	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::EMRServerless::Application	是	是	是	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::ElasticBeanstalk::Application	是	是	是	是	是	是	是	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::ElasticBeanstalk::ApplicationVersion	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ElasticBeanstalk::Environment	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ElasticLoadBalancing::LoadBalancer	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是	是	是	没有	是	是	是	是	是	没有	没有	是
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::ElasticLoadBalancingV2::TargetGroup	是	是	是	是	是	是	是	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Elasticsearch::Domain	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::EntityResolution::IdMapping工作流程	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::EntityResolution::MatchingWorkflow	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::EntityResolution::SchemaMapping	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::EventSchemas::Discoverer	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::EventSchemas::Registry	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::EventSchemas::RegistryPolicy	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::EventSchemas::Schema	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Events::ApiDestination	是	是	是	没有	没有	是	是	是	是	是	没有	是	是
AWS::Events::Archive	是	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Events::Connection	是	是	是	没有	没有	是	是	是	是	是	没有	是	是
AWS::Events::Endpoint	没有	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Events::EventBus	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Events::Rule	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::FIS::ExperimentTemplate	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Forecast::Dataset	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Forecast::DatasetGroup	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::FraudDetector::EntityType	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	没有
AWS::FraudDetector::Label	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	没有
AWS::FraudDetector::Outcome	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	没有
AWS::FraudDetector::Variable	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	没有
AWS::GameLift::Alias	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::GameLift::Build	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::GameLift::GameSession队列	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::GameLift::MatchmakingConfiguration	没有	没有	没有	没有	没有	没有	没有	是	没有	是	没有	没有	是
AWS::Glue::Classifier	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Glue::Database	是	是	是	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Glue::Job	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::Glue::MLTransform	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Glue::Registry	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Grafana::Workspace	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::GreengrassV2::ComponentVersion	没有	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::GroundStation::Config	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	没有
AWS::GroundStation::DataflowEndpoint群组	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	没有
AWS::GroundStation::MissionProfile	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	没有
AWS::GuardDuty::Detector	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::GuardDuty::Filter	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Guard职责:: IPSet	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::GuardDuty::MalwareProtection计划	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::GuardDuty::ThreatIntelSet	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Health湖::FHIRDatastore	没有	没有	没有	没有	没有	是	没有	没有	没有	没有	没有	没有	没有
AWS::IAM::Group	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::IAM::Policy	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::IAM::Role	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::IAM::User	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::IVS::Channel	没有	没有	没有	没有	没有	是	没有	是	没有	没有	没有	没有	是
AWS::IVS::PlaybackKey配对	没有	没有	没有	没有	没有	是	没有	是	没有	没有	没有	没有	是
AWS::IVS::RecordingConfiguration	没有	没有	没有	没有	没有	是	没有	是	没有	没有	没有	没有	是
AWS::ImageBuilder::ContainerRecipe	是	是	是	是	是	是	是	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::ImageBuilder::DistributionConfiguration	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ImageBuilder::ImagePipeline	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ImageBuilder::ImageRecipe	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ImageBuilder::InfrastructureConfiguration	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::ImageBuilder::LifecyclePolicy	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::InspectorV2::Activation	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::InspectorV2::Filter	是	是	是	是	没有	是	是	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::IoT::AccountAudit配置	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::Authorizer	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::CACertificate	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::CustomMetric	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::Dimension	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::DomainConfiguration	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::FleetMetric	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::JobTemplate	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::MitigationAction	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::IoT::Policy	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::ProvisioningTemplate	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::RoleAlias	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::ScheduledAudit	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::SecurityProfile	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoT::ThingGroup	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTAnalytics::Channel	没有	没有	没有	没有	没有	是	没有	没有	没有	是	没有	没有	是
AWS::IoTAnalytics::Dataset	没有	没有	没有	没有	没有	是	没有	没有	没有	是	没有	没有	是
AWS::IoTAnalytics::Datastore	没有	没有	没有	没有	没有	是	没有	没有	没有	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::IoTAnalytics::Pipeline	没有	没有	没有	没有	没有	是	没有	没有	没有	是	没有	没有	是
AWS::IoTCoreDeviceAdvisor::SuiteDefinition	没有	没有	没有	没有	没有	没有	没有	没有	没有	没有	没有	没有	是
AWS::IoTEvents::AlarmModel	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTEvents::DetectorModel	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTEvents::Input	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTSiteWise::Asset	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTSiteWise::AssetModel	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::IoTSiteWise::Dashboard	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTSiteWise::Gateway	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTSiteWise::Portal	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTSiteWise::Project	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTTwinMaker::ComponentType	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTTwinMaker::Entity	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	没有
AWS::IoTTwinMaker::Scene	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTTwinMaker::SyncJob	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::IoTTwinMaker::Workspace	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::IoTWireless::FuotaTask	没有	没有	没有	没有	没有	没有	没有	没有	没有	是	没有	没有	是
AWS::IoTWireless::MulticastGroup	没有	没有	没有	没有	没有	没有	没有	没有	没有	是	没有	没有	是
AWS::IoTWireless::ServiceProfile	没有	没有	没有	没有	没有	没有	没有	没有	没有	是	没有	没有	是
AWS::KMS::Alias	是	是	是	是	没有	是	是	是	是	是	没有	没有	是
AWS::KMS::Key	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::KafkaConnect::Connector	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::KafkaConnect::CustomPlugin	是	是	是	是	没有	是	没有	是	是	是	没有	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Kendra::Index	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是
AWS::Kinesis::Stream	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Kinesis::StreamConsumer	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::KinesisAnalyticsV2::Application	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::KinesisFirehose::DeliveryStream	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::KinesisVideo::SignalingChannel	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::KinesisVideo::Stream	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::Lambda::CodeSigningConfig	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Lambda::Function	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Lex::Bot	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Lex::BotAlias	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Lightsail::Bucket	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Lightsail::Certificate	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Lightsail::Disk	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Lightsail::StaticIp	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Location::APIKey	没有	没有	没有	没有	没有	是	没有	没有	是	是	没有	没有	是
AWS::Location::GeofenceCollection	没有	没有	没有	是	没有	是	没有	没有	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Location::Map	没有	没有	没有	是	没有	是	没有	没有	是	是	没有	没有	是
AWS::Location::PlaceIndex	没有	没有	没有	是	没有	是	没有	没有	是	是	没有	没有	是
AWS::Location::RouteCalculator	没有	没有	没有	是	没有	是	没有	没有	是	是	没有	没有	是
AWS::Logs::Destination	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::LookoutVision::Project	没有	没有	没有	没有	没有	没有	没有	是	没有	没有	没有	没有	是
AWS::M2::Environment	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::MSK::BatchScram秘密	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::MSK::Cluster	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::MSK::ClusterPolicy	是	是	是	没有	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::MSK::Configuration	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::MSK::ServerlessCluster	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::MSK::VpcConnection	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::Macie::Session	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::MediaConnect::FlowEntitlement	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaConnect::FlowSource	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaConnect::FlowVpc接口	是	是	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::MediaConnect::Gateway	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::MediaLive::Multiplexprogram	没有	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaPackage::Asset	没有	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaPackage::PackagingConfiguration	没有	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaPackage::PackagingGroup	没有	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaPackageV2::Channel	没有	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaPackageV2::ChannelGroup	没有	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaPackageV2::OriginEndpoint	没有	是	没有	没有	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::MediaTailor::LiveSource	没有	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MediaTailor::PlaybackConfiguration	没有	没有	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::MemoryDB::SubnetGroup	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::NetworkFirewall::Firewall	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::RuleGroup	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Network防火墙:: TLSInspection 配置	是	是	没有	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::NetworkFirewall::VpcEndpoint协会	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Omics::RunGroup	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	没有	没有
AWS::Omics::Workflow	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	没有	没有
AWS::OpenSearch::Domain	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::OpenSearchServerless::Collection	是	是	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::OpenSearchServerless::SecurityConfig	是	是	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::OpenSearchServerless::VpcEndpoint	是	是	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::PCAConnectorAD::Connector	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::PCAConnectorAD::DirectoryRegistration	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Panorama::Package	没有	没有	没有	没有	没有	没有	没有	没有	是	是	没有	没有	没有
AWS::Personalize::Dataset	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Personalize::DatasetGroup	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Personalize::Schema	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Personalize::Solution	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Pinpoint::App	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Pinpoint::ApplicationSettings	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Pinpoint::Campaign	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Pinpoint::EmailChannel	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Pinpoint::EmailTemplate	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Pinpoint::EventStream	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Pinpoint::InApp模板	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Pinpoint::Segment	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::QuickSight::Dashboard	没有	没有	是	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::QuickSight::DataSource	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::QuickSight::Template	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::QuickSight::Theme	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS:: RDS:: DBCluster	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:: RDS:: 快照 DBCluster	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:: RDS:: DBInstance	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:: RDS:: 终端节点 DBProxy	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS:: RDS:: 群组 DBSecurity	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS:: RDS:: DBSnapshot	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS:: RDS:: 群组 DBSubnet	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::RDS::EventSubscription	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::RDS::GlobalCluster	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::RDS::Integration	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::RDS::OptionGroup	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::RUM::AppMonitor	没有	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::Redshift::Cluster	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterParameter组	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSecurity组	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Redshift::ClusterSnapshot	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSubnet组	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::EndpointAccess	是	是	是	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::Redshift::EndpointAuthorization	是	是	是	是	没有	是	没有	是	是	是	没有	没有	是
AWS::Redshift::EventSubscription	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::Integration	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Redshift::ScheduledAction	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::ResilienceHub::App	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::ResilienceHub::ResiliencyPolicy	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::ResourceExplorer2::Index	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::RoboMaker::RobotApplication	没有	没有	没有	没有	没有	没有	没有	没有	是	没有	没有	没有	是
AWS::RoboMaker::RobotApplication版本	没有	没有	没有	没有	没有	没有	没有	没有	是	没有	没有	没有	是
AWS::RoboMaker::SimulationApplication	没有	没有	没有	没有	没有	没有	没有	没有	是	没有	没有	没有	是
AWS::Roles任何地方:: CRL	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::RolesAnywhere::Profile	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::RolesAnywhere::TrustAnchor	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Route53Profiles::Profile	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Route53Profiles::ProfileAssociation	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Route53Resolver::FirewallDomain清单	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::Route53Resolver::FirewallRule组	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Route53Resolver::ResolverEndpoint	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverRule	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Route53Resolver::ResolverRule协会	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::S3::AccessGrant	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::S3::AccessGrants实例	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::S3::AccessGrantsLocation	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::S3::AccessPoint	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::S3::AccountPublicAccessBlock	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::S3::Bucket	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::S3::StorageLens	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::S3::StorageLens组	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::S3Express::BucketPolicy	没有	没有	没有	没有	没有	是	没有	没有	没有	没有	没有	没有	是
AWS::S3Express::DirectoryBucket	没有	没有	没有	没有	没有	是	没有	没有	没有	没有	没有	没有	是
AWS::S3Tables::TableBucket	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::S3Tables::TableBucket政策	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::SES::ConfigurationSet	没有	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SES::ContactList	没有	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SES::DedicatedIp泳池	没有	是	是	没有	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::SES::MailManagerTrafficPolicy	没有	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SES::ReceiptFilter	没有	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SES::ReceiptRuleSet	没有	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SES::Template	没有	是	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SNS::Topic	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::SQS::Queue	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SSM::AssociationCompliance	是	是	是	是	是	是	没有	是	是	是	是	是	是
AWS::SSM::Document	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::SSM::FileData	是	是	是	是	是	是	没有	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::SSM::ManagedInstance 清单	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::SSM::PatchCompliance	是	是	是	是	是	是	没有	是	是	是	是	是	是
AWS::SSM::ResourceData同步	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::SSMContacts::Contact	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::SSMIncidents::ResponsePlan	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::SageMaker::AppImageConfig	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::CodeRepository	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::SageMaker::DataQualityJobDefinition	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::Domain	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::EndpointConfig	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::FeatureGroup	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::Image	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::InferenceExperiment	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::MlflowTracking服务器	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::SageMaker::Model	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::ModelBiasJobDefinition	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::ModelExplainabilityJobDefinition	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::ModelQualityJobDefinition	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::MonitoringSchedule	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::NotebookInstance	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	没有	没有	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::StudioLifecycleConfig	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::UserProfile	是	没有	是	没有	没有	是	是	是	是	是	没有	没有	是
AWS::SageMaker::Workteam	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::SecretsManager::ResourcePolicy	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::SecretsManager::RotationSchedule	是	是	是	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::SecretsManager::Secret	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::SecurityHub::Standard	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::ServiceCatalog::CloudFormation产品	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::ServiceCatalog::Portfolio	是	是	没有	没有	是	是	是	是	是	是	没有	没有	是
AWS::ServiceDiscovery::HttpNamespace	是	是	是	是	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::ServiceDiscovery::Instance	是	没有	是	是	没有	是	是	是	是	是	没有	没有	是
AWS::ServiceDiscovery::PublicDns命名空间	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::ServiceDiscovery::Service	是	没有	没有	是	没有	是	没有	是	是	是	没有	没有	是
AWS::ShieldRegional::Protection	是	是	是	是	是	是	是	是	是	是	没有	是	是
AWS::Signer::SigningProfile	是	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::StepFunctions::Activity	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::StepFunctions::StateMachine	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Transfer::Agreement	是	是	是	是	没有	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS::Transfer::Certificate	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Transfer::Connector	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Transfer::Profile	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Transfer::Server	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::Transfer::Workflow	是	是	是	是	是	是	是	是	是	是	没有	没有	是
AWS::WAFRegional::RateBased规则	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::WAFRegional::Rule	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::WAFRegional::RuleGroup	是	是	是	没有	是	是	是	是	是	是	没有	没有	是
AWS::WAFRegional::WebACL	是	是	是	没有	是	是	是	是	是	是	没有	没有	是

资源类型	亚太地区（香港）	亚太地区（海得拉巴）	亚太地区（雅加达）	亚太地区（马来西亚）	亚太地区（墨尔本）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（首尔）	亚太地区（新加坡）	亚太地区（悉尼）	亚太地区（台北）	亚太地区（泰国）	亚太地区（东京）
AWS:WAFv2 ::: IPSet	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::WAFv 2::Manage dRule设置	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::WAFv 2::RegexP attern设置	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::WAFv 2::RuleGroup	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::WAFv 2::WebACL	是	是	是	是	是	是	是	是	是	是	是	是	是
AWS::Work Spaces::C onnectionAlias	没有	没有	没有	没有	没有	没有	没有	是	是	是	没有	没有	是
AWS::Work Spaces::W orkspace	没有	没有	没有	没有	没有	是	没有	是	是	是	没有	没有	是
AWS::XRay ::EncryptionConfig	是	是	是	没有	是	是	是	是	是	是	是	是	是

中国区域

资源类型	中国（北京）	中国（宁夏）
AWS::ACM::Certificate	是	是
AWS::AmazonMQ::Broker	是	是
AWS::ApiGateway::DomainName	是	是
AWS::ApiGateway::Method	是	是
AWS::ApiGateway::RestApi	是	是
AWS::ApiGateway::Stage	是	是
AWS::ApiGateway::UsagePlan	是	是
AWS::ApiGatewayV2::Api	是	是
AWS::ApiGatewayV2::Integration	是	是
AWS::ApiGatewayV2::Stage	是	是
AWS::AppConfig::Application	是	是
AWS::AppConfig::ConfigurationProfile	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::AppConfig::DeploymentStrategy	是	是
AWS::AppConfig::Environment	是	是
AWS::AppConfig::Extension	是	是
AWS::AppConfig::ExtensionAssociation	是	是
AWS::AppConfig::HostedConfiguration版本	是	是
AWS::AppSync::Api	是	是
AWS::AppSync::ApiCache	是	是
AWS::AppSync::GraphQLApi	是	是
AWS::Athena::DataCatalog	是	是
AWS::Athena::PreparedStatement	是	是
AWS::Athena::WorkGroup	是	是
AWS::AutoScaling::AutoScaling组	是	是
AWS::AutoScaling::LaunchConfiguration	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::AutoScaling::ScalingPolicy	是	是
AWS::AutoScaling::ScheduledAction	是	是
AWS::AutoScaling::WarmPool	是	是
AWS::Backup::BackupPlan	是	是
AWS::Backup::BackupSelection	是	是
AWS::Backup::BackupVault	是	是
AWS::Backup::RecoveryPoint	是	是
AWS::Batch::ComputeEnvironment	是	是
AWS::Batch::JobQueue	是	是
AWS::Batch::SchedulingPolicy	是	是
AWS::Cassandra::Keyspace	是	是
AWS::CloudFormation::Stack	是	是
AWS::CloudFormation::StackSet	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::CloudFront::PublicKey	是	没有
AWS::CloudTrail::Trail	是	是
AWS::CloudWatch::Alarm	是	是
AWS::CloudWatch::MetricStream	是	是
AWS::CodeBuild::Project	是	是
AWS::CodeBuild::ReportGroup	是	是
AWS::Cognito::IdentityPool	是	没有
AWS::Config::AggregationAuthorization	是	是
AWS::Config::ConfigurationRecorder	是	是
AWS::Config::ResourceCompliance	是	是
AWS::Config::StoredQuery	是	是
AWS::DMS::Certificate	是	是
AWS::DMS::Endpoint	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::DMS::EventSubscription	是	是
AWS::DMS::ReplicationInstance	是	是
AWS::DMS::ReplicationSubnet组	是	是
AWS::DMS::ReplicationTask	是	是
AWS::DataSync::Agent	是	是
AWS::DataSync::LocationEFS	是	是
AWS::DataSync::LocationHDFS	是	是
AWS::DataSync::LocationNFS	是	是
AWS::DataSync::LocationObject存储	是	是
AWS::DataSync::LocationS3	是	是
AWS::DataSync::Location中小型企业	是	是
AWS::DataSync::Task	是	是
AWS::DynamoDB::Table	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EC2::CapacityReservation	是	是
AWS:EC2::: DHCPOptions	是	是
AWS:EC2:: EC2 舰队	是	是
AWS:::EC2: EIP	是	是
AWS:EC2::: EIPAssociation	是	是
AWS::EC2::FlowLog	是	是
AWS::EC2::Host	是	是
AWS::EC2::Instance	是	是
AWS::EC2::InternetGateway	是	是
AWS::EC2::LaunchTemplate	是	是
AWS::EC2::NatGateway	是	是
AWS::EC2::NetworkAcl	是	是
AWS::EC2::NetworkInterface	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EC2::PrefixList	是	是
AWS::EC2::RouteTable	是	是
AWS::EC2::SecurityGroup	是	是
AWS::EC2::SecurityGroupVpcAssociation	是	是
AWS::EC2::SnapshotBlockPublicAccess	是	是
AWS::EC2::SpotFleet	是	是
AWS::EC2::Subnet	是	是
AWS::EC2::SubnetCidr屏蔽	是	没有
AWS::EC2::SubnetNetworkAclAssociation	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是
AWS::EC2::TrafficMirror过滤器	是	是
AWS::EC2::TrafficMirrorSession	是	是
AWS::EC2::TrafficMirror目标	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EC2::TransitGateway	是	是
AWS::EC2::TransitGateway附件	是	是
AWS::EC2::TransitGatewayConnect	是	是
AWS::EC2::TransitGatewayMulticastDomain	是	是
AWS::EC2::TransitGatewayRouteTable	是	是
AWS:::EC2: VPC	是	是
AWS:EC2::: VPCBlock PublicAccessExclusion	是	是
AWS:EC2::: VPCBlock PublicAccessOptions	是	是
AWS:EC2::: VPCEndpoint	是	是
AWS:EC2::: VPCEndpoint ConnectionNotification	是	是
AWS:EC2::: VPCEndpoint 服务	是	是
AWS::EC2:: VPCGateway 附件	是	是
AWS:EC2:: VPCPeering 连接	是	是

资源类型	中国（北京）	中国（宁夏）
AWS:EC2::: VPNGateway	是	没有
AWS::EC2::Volume	是	是
AWS::ECR::ReplicationConfiguration	是	是
AWS::ECR::Repository	是	是
AWS::ECS::CapacityProvider	是	是
AWS::ECS::Cluster	是	是
AWS::ECS::Service	是	是
AWS::ECS::TaskDefinition	是	是
AWS::ECS::TaskSet	是	是
AWS::EFS::AccessPoint	是	是
AWS::EFS::FileSystem	是	是
AWS::EKS::Addon	是	是
AWS::EKS::Cluster	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EKS::FargateProfile	是	是
AWS::EKS::IdentityProviderConfig	是	是
AWS::EMR::SecurityConfiguration	是	是
AWS::EMR::Studio	是	是
AWS::EMRContainers::VirtualCluster	是	是
AWS::EMRServerless::Application	是	是
AWS::ElasticBeanstalk::Application	是	是
AWS::ElasticBeanstalk::ApplicationVersion	是	是
AWS::ElasticBeanstalk::Environment	是	是
AWS::ElasticLoadBalancing::LoadBalancer	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是
AWS::ElasticLoadBalancingV2::TargetGroup	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Elasticsearch::Domain	是	是
AWS::Events::Archive	是	是
AWS::Events::EventBus	是	是
AWS::Events::Rule	是	是
AWS::GameLift::Alias	是	是
AWS::GameLift::GameSession队列	是	是
AWS::GameLift::MatchmakingConfiguration	是	是
AWS::Glue::Classifier	是	是
AWS::Glue::Job	是	是
AWS::Glue::MLTransform	是	没有
AWS::Glue::Registry	是	是
AWS::GreengrassV2::ComponentVersion	是	没有
AWS::GuardDuty::Filter	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::GuardDuty::ThreatIntelSet	是	是
AWS::IAM::Group	是	是
AWS::IAM::InstanceProfile	是	没有
AWS:: IAM:: OIDCProvider	是	没有
AWS::IAM::Policy	是	是
AWS::IAM::Role	是	是
AWS:: IAM:: SAMLProvider	是	没有
AWS::IAM::ServerCertificate	是	没有
AWS::IAM::User	是	是
AWS::ImageBuilder::ContainerRecipe	是	是
AWS::ImageBuilder::DistributionConfiguration	是	是
AWS::ImageBuilder::ImagePipeline	是	是
AWS::ImageBuilder::ImageRecipe	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::ImageBuilder::InfrastructureConfiguration	是	是
AWS::InspectorV2::Activation	是	是
AWS::IoT::AccountAudit配置	是	是
AWS::IoT::Authorizer	是	是
AWS::IoT:: CACertificate	是	是
AWS::IoT::CustomMetric	是	是
AWS::IoT::Dimension	是	是
AWS::IoT::DomainConfiguration	是	是
AWS::IoT::FleetMetric	是	是
AWS::IoT::JobTemplate	是	是
AWS::IoT::MitigationAction	是	是
AWS::IoT::Policy	是	是
AWS::IoT::ProvisioningTemplate	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::IoT::RoleAlias	是	是
AWS::IoT::ScheduledAudit	是	是
AWS::IoT::SecurityProfile	是	是
AWS::IoT::ThingGroup	是	是
AWS::IoTAnalytics::Channel	是	没有
AWS::IoTAnalytics::Dataset	是	没有
AWS::IoTAnalytics::Datastore	是	没有
AWS::IoTAnalytics::Pipeline	是	没有
AWS::IoTEvents::AlarmModel	是	没有
AWS::IoTEvents::DetectorModel	是	没有
AWS::IoTEvents::Input	是	没有
AWS::IoTSiteWise::Asset	是	没有
AWS::IoTSiteWise::AssetModel	是	没有

资源类型	中国（北京）	中国（宁夏）
AWS::IoTSiteWise::Dashboard	是	没有
AWS::IoTSiteWise::Gateway	是	没有
AWS::IoTSiteWise::Portal	是	没有
AWS::IoTSiteWise::Project	是	没有
AWS::KMS::Alias	是	是
AWS::KMS::Key	是	是
AWS::Kinesis::Stream	是	是
AWS::Kinesis::StreamConsumer	是	是
AWS::KinesisAnalyticsV2::Application	是	是
AWS::KinesisFirehose::DeliveryStream	是	是
AWS::Lambda::Function	是	没有
AWS::Logs::Destination	是	是
AWS::MSK::BatchScram秘密	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::MSK::Cluster	是	是
AWS::MSK::ClusterPolicy	是	是
AWS::MSK::Configuration	是	是
AWS::MSK::VpcConnection	是	是
AWS::NetworkFirewall::Firewall	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是
AWS::NetworkFirewall::RuleGroup	是	是
AWS::Network防火墙:: TLSInspection 配置	是	是
AWS::NetworkFirewall::VpcEndpoint协会	是	是
AWS::OpenSearch::Domain	是	是
AWS::Personalize::Dataset	是	没有
AWS::Personalize::DatasetGroup	是	没有
AWS::Personalize::Schema	是	没有

资源类型	中国（北京）	中国（宁夏）
AWS::Personalize::Solution	是	没有
AWS::QuickSight::Dashboard	是	没有
AWS:: RDS:: DBCluster	没有	是
AWS:: RDS:: 快照 DBCluster	是	是
AWS:: RDS:: DBInstance	是	是
AWS:: RDS:: 终端节点 DBProxy	是	是
AWS:: RDS:: 群组 DBSecurity	是	是
AWS:: RDS:: DBSnapshot	是	是
AWS:: RDS:: 群组 DBSubnet	是	是
AWS::RDS::EventSubscription	是	是
AWS::RDS::Integration	是	是
AWS::RDS::OptionGroup	是	是
AWS::Redshift::Cluster	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Redshift::ClusterParameter组	是	是
AWS::Redshift::ClusterSecurity组	是	是
AWS::Redshift::ClusterSnapshot	是	是
AWS::Redshift::ClusterSubnet组	是	是
AWS::Redshift::EventSubscription	是	是
AWS::Redshift::Integration	是	是
AWS::Roles任何地方:: CRL	是	是
AWS::RolesAnywhere::Profile	是	是
AWS::RolesAnywhere::TrustAnchor	是	是
AWS::Route53Profiles::Profile	是	是
AWS::Route53Profiles::ProfileAssociation	是	是
AWS::Route53Resolver::FirewallDomain清单	是	是
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Route53Resolver::ResolverEndpoint	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	是	是
AWS::Route53Resolver::ResolverRule	是	是
AWS::Route53Resolver::ResolverRule协会	是	是
AWS::S3::AccessGrant	是	是
AWS::S3::AccessGrants实例	是	是
AWS::S3::AccessGrantsLocation	是	是
AWS::S3::AccessPoint	是	是
AWS::S3::AccountPublicAccessBlock	是	是
AWS::S3::Bucket	是	是
AWS::S3::StorageLens组	是	是
AWS::SES::ConfigurationSet	没有	是

资源类型	中国（北京）	中国（宁夏）
AWS::SES::ContactList	没有	是
AWS::SES::Template	没有	是
AWS::SNS::Topic	是	是
AWS::SQS::Queue	是	是
AWS::SSM::AssociationCompliance	是	是
AWS::SSM::Document	是	是
AWS::SSM::FileData	是	是
AWS::SSM::ManagedInstance 清单	是	是
AWS::SSM::PatchCompliance	是	是
AWS::SSM::ResourceData同步	是	是
AWS::SageMaker::AppImageConfig	是	是
AWS::SageMaker::CodeRepository	是	是
AWS::SageMaker::Domain	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::SageMaker::EndpointConfig	是	是
AWS::SageMaker::FeatureGroup	是	是
AWS::SageMaker::Image	是	是
AWS::SageMaker::Model	是	是
AWS::SageMaker::MonitoringSchedule	是	是
AWS::SageMaker::NotebookInstance	是	是
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	是
AWS::SageMaker::StudioLifecycleConfig	是	是
AWS::SageMaker::UserProfile	是	是
AWS::SecretsManager::ResourcePolicy	是	是
AWS::SecretsManager::RotationSchedule	是	是
AWS::SecretsManager::Secret	是	是
AWS::SecurityHub::Standard	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::ServiceCatalog::CloudFormation产品	是	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是
AWS::ServiceCatalog::Portfolio	是	是
AWS::ServiceDiscovery::HttpNamespace	是	是
AWS::ServiceDiscovery::Instance	是	是
AWS::ServiceDiscovery::PublicDns命名空间	是	是
AWS::ServiceDiscovery::Service	是	是
AWS::StepFunctions::Activity	是	没有
AWS::StepFunctions::StateMachine	是	是
AWS::Transfer::Agreement	是	是
AWS::Transfer::Certificate	是	是
AWS::Transfer::Connector	是	是
AWS::Transfer::Profile	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Transfer::Server	是	是
AWS::Transfer::Workflow	是	是
AWS::WAFRegional::RateBased规则	是	是
AWS::WAFRegional::Rule	是	是
AWS::WAFRegional::RuleGroup	是	是
AWS::WAFRegional::WebACL	是	是
AWS:WAFv2::: IPSet	是	是
AWS::WAFv2::ManagedRuleSet	是	是
AWS::WAFv2::RegexPatternSet	是	是
AWS::WAFv2::RuleGroup	是	是
AWS::WAFv2::WebACL	是	是
AWS::WorkSpaces::Workspace	没有	是

非洲和中东区域

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::ACM::Certificate	是	是	是	是
AWS::ACMPCA::CertificateAuthority	是	是	是	是
AWS::ACMPCA::CertificateAuthority激活	是	是	是	是
AWS::APS::RuleGroups命名空间	是	没有	是	是
AWS::AccessAnalyzer::Analyzer	是	是	是	是
AWS::AmazonMQ::Broker	是	没有	是	是
AWS::Amplify::App	没有	没有	是	没有
AWS::Amplify::Branch	没有	没有	是	没有
AWS::ApiGateway::DomainName	是	是	是	是
AWS::ApiGateway::Method	是	是	是	是
AWS::ApiGateway::RestApi	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::ApiGateway::Stage	是	是	是	是
AWS::ApiGateway::UsagePlan	是	是	是	是
AWS::ApiGatewayV2::Api	是	是	是	是
AWS::ApiGatewayV2::Integration	是	是	是	是
AWS::ApiGatewayV2::Stage	是	是	是	是
AWS::AppConfig::Application	是	是	是	没有
AWS::AppConfig::ConfigurationProfile	是	是	是	没有
AWS::AppConfig::DeploymentStrategy	是	是	是	是
AWS::AppConfig::Environment	是	是	是	没有
AWS::AppConfig::Extension	是	是	是	是
AWS::AppConfig::ExtensionAssociation	是	是	是	是
AWS::AppConfig::HostedConfiguration版本	是	是	是	没有

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::AppFlow::Flow	是	没有	没有	没有
AWS::AppIntegrations::Application	是	没有	没有	没有
AWS::AppIntegrations::DataIntegration	是	没有	没有	没有
AWS::AppIntegrations::EventIntegration	是	没有	没有	没有
AWS::AppMesh::GatewayRoute	是	是	是	没有
AWS::AppMesh::Mesh	是	是	是	没有
AWS::AppMesh::Route	是	是	是	没有
AWS::AppMesh::VirtualGateway	是	是	是	没有
AWS::AppMesh::VirtualNode	是	是	是	没有
AWS::AppMesh::VirtualRouter	是	是	是	没有
AWS::AppMesh::VirtualService	是	是	是	没有
AWS::AppSync::Api	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::AppSync::ApiCache	是	是	是	是
AWS::AppSync::GraphQLApi	是	是	是	是
AWS::Athena::DataCatalog	是	是	是	是
AWS::Athena::PreparedStatement	是	是	是	是
AWS::Athena::WorkGroup	是	是	是	是
AWS::AutoScaling::AutoScaling组	是	是	是	是
AWS::AutoScaling::LaunchConfiguration	是	是	是	是
AWS::AutoScaling::ScalingPolicy	是	是	是	是
AWS::AutoScaling::ScheduledAction	是	是	是	是
AWS::AutoScaling::WarmPool	是	没有	是	没有
AWS::Backup::BackupPlan	是	是	是	是
AWS::Backup::BackupSelection	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::Backup::BackupVault	是	是	是	是
AWS::Backup::RecoveryPoint	是	是	是	是
AWS::Backup::ReportPlan	是	没有	是	是
AWS::Backup::RestoreTesting计划	是	没有	是	是
AWS::BackupGateway::Hypervisor	是	没有	是	没有
AWS::Batch::ComputeEnvironment	是	没有	是	是
AWS::Batch::JobQueue	是	没有	是	是
AWS::Batch::SchedulingPolicy	是	是	是	是
AWS::Bedrock::Guardrail	没有	没有	没有	是
AWS::Cassandra::Keyspace	没有	没有	是	没有
AWS::Cloud9::EnvironmentEC2	是	没有	是	没有
AWS::CloudFormation::GuardHook	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::CloudFormation::LambdaHook	是	是	是	是
AWS::CloudFormation::Stack	是	没有	是	没有
AWS::CloudFormation::StackSet	是	是	是	是
AWS::CloudTrail::EventData商店	是	是	是	是
AWS::CloudTrail::Trail	是	是	是	是
AWS::CloudWatch::Alarm	是	是	是	是
AWS::CloudWatch::MetricStream	是	是	是	是
AWS::CodeBuild::Project	是	是	是	是
AWS::CodeBuild::ReportGroup	是	是	是	是
AWS::CodeDeploy::Application	是	没有	是	没有
AWS::CodeDeploy::DeploymentConfig	是	没有	是	没有
AWS::CodeDeploy::DeploymentGroup	是	没有	是	没有

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::CodePipeline::Pipeline	没有	是	没有	是
AWS::Cognito::IdentityPool	是	是	是	是
AWS::Cognito::UserPool	是	是	是	是
AWS::Cognito::UserPool客户端	是	是	是	是
AWS::Cognito::UserPool组	是	是	是	是
AWS::Config::AggregationAuthorization	是	是	是	是
AWS::Config::ConfigurationRecorder	是	是	是	是
AWS::Config::ConformancePack	是	是	是	是
AWS::Config::Confo rmancePack Compliance	是	是	是	是
AWS::Config::ResourceCompliance	是	是	是	是
AWS::Config::StoredQuery	是	是	是	是
AWS::Connect::Instance	是	没有	没有	没有

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::Connect::PhoneNumber	是	没有	没有	没有
AWS::Connect::QuickConnect	是	没有	没有	没有
AWS::Connect::Rule	是	没有	没有	没有
AWS::Connect::SecurityProfile	是	没有	没有	没有
AWS::Connect::User	是	没有	没有	没有
AWS::CustomerProfiles::Domain	是	没有	没有	没有
AWS::CustomerProfiles::ObjectType	是	没有	没有	没有
AWS::DMS::Certificate	是	没有	是	没有
AWS::DMS::Endpoint	是	没有	是	没有
AWS::DMS::EventSubscription	是	没有	是	没有
AWS::DMS::MigrationProject	是	是	是	是
AWS::DMS::ReplicationInstance	是	没有	是	没有

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::DMS::ReplicationSubnet组	是	没有	是	没有
AWS::DMS::ReplicationTask	是	没有	是	没有
AWS::DataSync::Agent	是	是	是	是
AWS::DataSync::LocationEFS	是	没有	是	是
AWS::DataSync::LocationFSxLustre	是	没有	是	是
AWS::DataSync::LocationFSx窗户	是	没有	是	没有
AWS::DataSync::LocationHDFS	是	没有	是	是
AWS::DataSync::LocationNFS	是	没有	是	是
AWS::DataSync::LocationObject存储	是	没有	是	是
AWS::DataSync::LocationS3	是	是	是	是
AWS::DataSync::Location中小型企业	是	没有	是	是
AWS::DataSync::Task	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::Detective::Graph	是	是	是	没有
AWS::DynamoDB::Table	是	是	是	是
AWS::EC2::CapacityReservation	是	是	是	是
AWS::EC2::ClientVpn端点	是	没有	是	是
AWS::EC2::ClientVpnTargetNetworkAssociation	是	是	是	是
AWS::EC2::CustomerGateway	是	是	是	是
AWS:EC2::: DHCPOptions	是	是	是	是
AWS:EC2:: EC2 舰队	是	没有	是	是
AWS:::EC2: EIP	是	是	是	是
AWS:EC2::: EIPAssociation	是	是	是	是
AWS::EC2::EgressOnlyInternetGateway	是	没有	是	是
AWS::EC2::FlowLog	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::EC2::Host	是	是	是	是
AWS:::EC2: IPAM	是	没有	是	是
AWS:EC2::: IPAMPool	是	没有	是	是
AWS::EC2:: IPAMPool Cidr	是	是	是	是
AWS::EC2: IPAMResource Discovery	是	是	是	是
AWS:EC2::: IPAMResource DiscoveryAssociation	是	是	是	是
AWS:EC2::: IPAMScope	是	没有	是	是
AWS::EC2::Instance	是	是	是	是
AWS::EC2::InstanceConnect端点	是	是	是	是
AWS::EC2::InternetGateway	是	是	是	是
AWS::EC2::LaunchTemplate	是	没有	是	没有
AWS::EC2::NatGateway	是	没有	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::EC2::NetworkAcl	是	是	是	是
AWS::EC2::NetworkInsightsAccessScope	是	没有	是	是
AWS::EC2::NetworkInsightsAccessScopeAnalysis	是	没有	是	是
AWS::EC2::NetworkInsights分析	是	没有	是	没有
AWS::EC2::NetworkInsights路径	是	没有	是	是
AWS::EC2::NetworkInterface	是	是	是	是
AWS::EC2::PrefixList	是	是	是	是
AWS::EC2::RouteTable	是	是	是	是
AWS::EC2::SecurityGroup	是	是	是	是
AWS::EC2::SecurityGroupVpcAssociation	是	是	是	是
AWS::EC2::SnapshotBlockPublicAccess	是	是	是	是
AWS::EC2::SpotFleet	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::EC2::Subnet	是	是	是	是
AWS::EC2::SubnetCidr屏蔽	是	是	是	是
AWS::EC2::SubnetNetworkAclAssociation	是	是	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是	是	是
AWS::EC2::TrafficMirror过滤器	是	是	是	是
AWS::EC2::TrafficMirrorSession	是	没有	是	是
AWS::EC2::TrafficMirror目标	是	没有	是	是
AWS::EC2::TransitGateway	是	是	是	是
AWS::EC2::TransitGateway附件	是	没有	是	是
AWS::EC2::TransitGatewayConnect	是	没有	是	是
AWS::EC2::TransitGatewayMulticastDomain	是	是	是	是
AWS::EC2::TransitGatewayRouteTable	是	没有	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS:::EC2: VPC	是	是	是	是
AWS:EC2::: VPCBlock PublicAccessExclusion	是	是	是	是
AWS:EC2::: VPCBlock PublicAccessOptions	是	是	是	是
AWS:EC2::: VPCEndpoint	是	是	是	是
AWS:EC2::: VPCEndpoi nt ConnectionNotification	是	是	是	是
AWS:EC2::: VPCEndpoint 服务	是	是	是	是
AWS::EC2:: VPCGateway 附件	是	是	是	是
AWS:EC2:: VPCPeering 连接	是	是	是	是
AWS:EC2::: VPNConnection	是	是	是	是
AWS::EC2:: VPNConnection 路线	是	是	是	是
AWS:EC2::: VPNGateway	是	是	是	是
AWS::EC2::VerifiedAccess实例	没有	是	没有	没有

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::EC2::Volume	是	是	是	是
AWS::ECR::PullThroughCacheRule	是	是	是	是
AWS::ECR::RegistryPolicy	是	是	是	是
AWS::ECR::ReplicationConfiguration	是	是	是	是
AWS::ECR::Repository	是	是	是	是
AWS::ECR::RepositoryCreation模板	是	是	是	是
AWS::ECS::CapacityProvider	是	是	是	是
AWS::ECS::Cluster	是	是	是	是
AWS::ECS::Service	是	是	是	是
AWS::ECS::TaskDefinition	是	是	是	是
AWS::ECS::TaskSet	是	没有	是	是
AWS::EFS::AccessPoint	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::EFS::FileSystem	是	是	是	是
AWS::EKS::Addon	是	没有	是	是
AWS::EKS::Cluster	是	是	是	是
AWS::EKS::FargateProfile	是	是	是	是
AWS::EKS::IdentityProviderConfig	是	没有	是	是
AWS::EMR::SecurityConfiguration	是	是	是	是
AWS::EMR::Studio	是	是	是	是
AWS::EMRContainers::VirtualCluster	是	是	是	是
AWS::EMRServerless::Application	是	没有	是	是
AWS::ElasticBeanstalk::Application	是	没有	是	是
AWS::ElasticBeanstalk::ApplicationVersion	是	没有	是	是
AWS::ElasticBeanstalk::Environment	是	没有	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::ElasticLoadBalancing::LoadBalancer	是	是	是	是
AWS::ElasticLoadBalancingV2::Listener	是	没有	是	是
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是	是	是
AWS::ElasticLoadBalancingV2::TargetGroup	是	是	是	是
AWS::Elasticsearch::Domain	是	是	是	是
AWS::EntityResolution::IdMapping工作流程	是	没有	没有	没有
AWS::EntityResolution::MatchingWorkflow	是	没有	没有	没有
AWS::EntityResolution::SchemaMapping	是	没有	没有	没有
AWS::EventSchemas::Discoverer	是	没有	是	是
AWS::EventSchemas::Registry	是	没有	是	是
AWS::EventSchemas::RegistryPolicy	是	没有	是	是
AWS::EventSchemas::Schema	是	没有	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::Events::ApiDestination	是	没有	是	是
AWS::Events::Archive	是	没有	是	是
AWS::Events::Connection	是	没有	是	是
AWS::Events::EventBus	是	是	是	是
AWS::Events::Rule	是	没有	是	没有
AWS::FIS::ExperimentTemplate	是	没有	是	没有
AWS::Glue::Classifier	是	是	是	是
AWS::Glue::Database	是	没有	是	是
AWS::Glue::Job	是	是	是	是
AWS::Glue::MLTransform	是	是	是	是
AWS::Glue::Registry	是	没有	是	没有
AWS::GroundStation::Config	是	没有	是	没有

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::GroundStation::DataflowEndpoint组	是	没有	是	没有
AWS::GroundStation::MissionProfile	是	没有	是	没有
AWS::GuardDuty::Detector	是	是	是	是
AWS::GuardDuty::Filter	是	没有	是	没有
AWS::Guard职责:: IPSet	是	没有	是	是
AWS::GuardDuty::MalwareProtection计划	是	是	是	是
AWS::GuardDuty::ThreatIntelSet	是	是	是	是
AWS::IAM::Group	是	没有	是	没有
AWS::IAM::Policy	是	没有	是	没有
AWS::IAM::Role	是	没有	是	没有
AWS::IAM::User	是	没有	是	没有
AWS::ImageBuilder::ContainerRecipe	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::ImageBuilder::DistributionConfiguration	是	是	是	是
AWS::ImageBuilder::ImagePipeline	是	是	是	是
AWS::ImageBuilder::ImageRecipe	是	是	是	是
AWS::ImageBuilder::InfrastructureConfiguration	是	是	是	是
AWS::ImageBuilder::LifecyclePolicy	是	没有	是	是
AWS::InspectorV2::Activation	是	是	是	是
AWS::InspectorV2::Filter	是	没有	是	是
AWS::IoT::AccountAudit配置	没有	没有	是	是
AWS::IoT::Authorizer	没有	没有	是	是
AWS::IoT:: CACertificate	没有	没有	是	是
AWS::IoT::CustomMetric	没有	没有	是	是
AWS::IoT::Dimension	没有	没有	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::IoT::DomainConfiguration	没有	没有	是	是
AWS::IoT::FleetMetric	没有	没有	是	是
AWS::IoT::JobTemplate	没有	没有	是	是
AWS::IoT::MitigationAction	没有	没有	是	是
AWS::IoT::Policy	没有	没有	是	是
AWS::IoT::ProvisioningTemplate	没有	没有	是	是
AWS::IoT::RoleAlias	没有	没有	是	是
AWS::IoT::ScheduledAudit	没有	没有	是	是
AWS::IoT::SecurityProfile	没有	没有	是	是
AWS::IoT::ThingGroup	没有	没有	是	是
AWS::KMS::Alias	是	没有	是	是
AWS::KMS::Key	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::KafkaConnect::CustomPlugin	是	没有	是	是
AWS::Kinesis::Stream	是	没有	是	是
AWS::Kinesis::StreamConsumer	是	是	是	是
AWS::KinesisAnalyticsV2::Application	是	是	是	是
AWS::KinesisFirehose::DeliveryStream	是	是	是	是
AWS::KinesisVideo::SignalingChannel	没有	没有	是	没有
AWS::KinesisVideo::Stream	没有	没有	是	没有
AWS::Lambda::CodeSigningConfig	是	没有	是	没有
AWS::Lambda::Function	是	是	是	是
AWS::Lex::Bot	是	没有	没有	没有
AWS::Lex::BotAlias	是	没有	没有	没有
AWS::Logs::Destination	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::MSK::BatchScram秘密	是	没有	是	是
AWS::MSK::Cluster	是	没有	是	是
AWS::MSK::ClusterPolicy	是	是	是	是
AWS::MSK::Configuration	是	是	是	是
AWS::MSK::VpcConnection	是	是	是	是
AWS::Macie::Session	是	是	是	没有
AWS::MediaConnect::FlowEntitlement	是	没有	没有	是
AWS::MediaConnect::FlowSource	是	没有	没有	是
AWS::MediaConnect::FlowVpc接口	是	没有	没有	是
AWS::MediaConnect::Gateway	是	没有	没有	没有
AWS::MediaLive::Multiplexprogram	没有	没有	没有	是
AWS::MediaPackage::Asset	没有	没有	没有	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::MediaPackage::PackagingConfiguration	没有	没有	没有	是
AWS::MediaPackage::PackagingGroup	没有	没有	没有	是
AWS::MediaPackageV2::Channel	没有	没有	没有	是
AWS::MediaPackageV2::ChannelGroup	没有	没有	没有	是
AWS::MediaPackageV2::OriginEndpoint	没有	没有	没有	是
AWS::MediaTailor::LiveSource	是	没有	没有	是
AWS::MediaTailor::PlaybackConfiguration	是	没有	没有	是
AWS::NetworkFirewall::Firewall	是	是	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是	是	是
AWS::NetworkFirewall::RuleGroup	是	是	是	是
AWS::Network防火墙:: TLSInspection 配置	是	是	是	是
AWS::NetworkFirewall::VpcEndpoint协会	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::Omics::RunGroup	没有	是	没有	没有
AWS::Omics::Workflow	没有	是	没有	没有
AWS::OpenSearch::Domain	是	没有	是	没有
AWS::PCAConnectorAD::Connector	是	是	是	是
AWS::PCAConnectorAD::DirectoryRegistration	是	是	是	是
AWS::QuickSight::Dashboard	是	没有	没有	没有
AWS:: RDS:: DBCluster	是	是	是	是
AWS:: RDS:: 快照 DBCluster	是	没有	是	是
AWS:: RDS:: DBInstance	是	是	是	是
AWS:: RDS:: 终端节点 DBProxy	是	是	是	是
AWS:: RDS:: 群组 DBSecurity	是	是	是	是
AWS:: RDS:: DBSnapshot	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS:: RDS:: 群组 DBSubnet	是	是	是	是
AWS::RDS::EventSubscription	是	是	是	是
AWS::RDS::GlobalCluster	是	是	是	是
AWS::RDS::Integration	是	是	是	是
AWS::RDS::OptionGroup	是	是	是	是
AWS::RUM::AppMonitor	是	没有	是	是
AWS::Redshift::Cluster	是	是	是	是
AWS::Redshift::ClusterParameter组	是	是	是	是
AWS::Redshift::ClusterSecurity组	是	是	是	是
AWS::Redshift::ClusterSnapshot	是	是	是	是
AWS::Redshift::ClusterSubnet组	是	是	是	是
AWS::Redshift::EndpointAccess	是	没有	是	没有

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::Redshift::EndpointAuthorization	是	没有	是	没有
AWS::Redshift::EventSubscription	是	是	是	是
AWS::Redshift::Integration	是	是	是	是
AWS::Redshift::ScheduledAction	没有	没有	是	没有
AWS::ResilienceHub::App	是	没有	是	没有
AWS::ResilienceHub::ResiliencyPolicy	是	没有	是	没有
AWS::ResourceExplorer2::Index	是	没有	是	是
AWS::Roles任何地方:: CRL	是	是	是	是
AWS::RolesAnywhere::Profile	是	是	是	是
AWS::RolesAnywhere::TrustAnchor	是	是	是	是
AWS::Route53Profiles::Profile	是	是	是	是
AWS::Route53Profiles::ProfileAssociation	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::Route53Resolver::FirewallDomain清单	是	没有	是	没有
AWS::Route53Resolver::FirewallRule组	是	没有	是	没有
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是	是	是
AWS::Route53Resolver::ResolverEndpoint	是	没有	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	是	是	是	是
AWS::Route53Resolver::ResolverRule	是	没有	是	是
AWS::Route53Resolver::ResolverRule协会	是	没有	是	是
AWS::S3::AccessGrant	是	是	是	是
AWS::S3::AccessGrants实例	是	是	是	是
AWS::S3::AccessGrantsLocation	是	是	是	是
AWS::S3::AccessPoint	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::S3::AccountPublicAccessBlock	是	没有	是	是
AWS::S3::Bucket	是	是	是	是
AWS::S3Tables::TableBucket	是	是	是	是
AWS::S3Tables::TableBucket政策	是	是	是	是
AWS::SES::ConfigurationSet	是	是	是	是
AWS::SES::ContactList	是	是	是	是
AWS::SES::DedicatedIp泳池	是	是	是	是
AWS::SES::MailManagerTrafficPolicy	是	没有	是	是
AWS::SES::ReceiptFilter	是	没有	是	没有
AWS::SES::ReceiptRuleSet	是	没有	是	没有
AWS::SES::Template	是	是	是	是
AWS::SNS::Topic	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::SQS::Queue	是	没有	是	没有
AWS::SSM::AssociationCompliance	是	是	是	是
AWS::SSM::Document	是	是	是	是
AWS::SSM::FileData	是	是	是	是
AWS::SSM::ManagedInstance 清单	是	是	是	是
AWS::SSM::PatchCompliance	是	是	是	是
AWS::SSM::ResourceData同步	是	是	是	是
AWS::SageMaker::AppImageConfig	是	是	是	是
AWS::SageMaker::CodeRepository	是	没有	是	没有
AWS::SageMaker::DataQualityJobDefinition	没有	没有	是	没有
AWS::SageMaker::Domain	是	没有	是	没有
AWS::SageMaker::EndpointConfig	是	没有	是	没有

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::SageMaker::FeatureGroup	是	是	是	没有
AWS::SageMaker::Image	是	是	是	是
AWS::SageMaker::InferenceExperiment	是	没有	是	没有
AWS::SageMaker::MlflowTracking服务器	是	是	是	是
AWS::SageMaker::Model	是	没有	是	没有
AWS::SageMaker::ModelBiasJobDefinition	没有	没有	是	没有
AWS::SageMaker::ModelExplainabilityJobDefinition	没有	没有	是	没有
AWS::SageMaker::ModelQualityJobDefinition	没有	没有	是	没有
AWS::SageMaker::MonitoringSchedule	没有	没有	是	没有
AWS::SageMaker::NotebookInstance	是	没有	是	没有
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	没有	是	没有
AWS::SageMaker::StudioLifecycleConfig	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::SageMaker::UserProfile	是	是	是	是
AWS::SecretsManager::ResourcePolicy	是	是	是	是
AWS::SecretsManager::RotationSchedule	是	是	是	是
AWS::SecretsManager::Secret	是	是	是	是
AWS::SecurityHub::Standard	是	是	是	是
AWS::ServiceCatalog::CloudFormation产品	是	没有	是	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	没有	是	是
AWS::ServiceCatalog::Portfolio	是	没有	是	是
AWS::ServiceDiscovery::HttpNamespace	是	是	是	是
AWS::ServiceDiscovery::Instance	是	没有	是	是
AWS::ServiceDiscovery::PublicDns命名空间	是	是	是	是
AWS::ServiceDiscovery::Service	是	没有	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::ShieldRegional::Protection	是	是	是	是
AWS::Signer::SigningProfile	是	没有	是	没有
AWS::StepFunctions::Activity	是	是	是	是
AWS::StepFunctions::StateMachine	是	是	是	是
AWS::Transfer::Agreement	是	没有	是	是
AWS::Transfer::Certificate	是	是	是	是
AWS::Transfer::Connector	是	是	是	是
AWS::Transfer::Profile	是	是	是	是
AWS::Transfer::Server	是	是	是	是
AWS::Transfer::Workflow	是	是	是	是
AWS::WAFRegional::RateBased规则	是	是	是	是
AWS::WAFRegional::Rule	是	是	是	是

资源类型	非洲（开普敦）	以色列（特拉维夫）	中东（巴林）	中东（阿联酋）：
AWS::WAFRegional::RuleGroup	是	是	是	是
AWS::WAFRegional::WebACL	是	是	是	是
AWS:WAFv2::: IPSet	是	是	是	是
AWS::WAFv2::ManagedRuleSet	是	是	是	是
AWS::WAFv2::RegexPatternSet	是	是	是	是
AWS::WAFv2::RuleGroup	是	是	是	是
AWS::WAFv2::WebACL	是	是	是	是
AWS::WorkSpaces::Workspace	是	没有	没有	没有
AWS::XRay::EncryptionConfig	是	是	没有	是

GovCloud 区域

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::ACM::Certificate	是	是
AWS::ACMPCA::CertificateAuthority	是	是
AWS::ACMPCA::CertificateAuthority激活	是	是
AWS::AccessAnalyzer::Analyzer	是	是
AWS::AmazonMQ::Broker	是	是
AWS::ApiGateway::DomainName	是	是
AWS::ApiGateway::Method	是	是
AWS::ApiGateway::RestApi	是	是
AWS::ApiGateway::Stage	是	是
AWS::ApiGateway::UsagePlan	是	是
AWS::ApiGatewayV2::Api	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::ApiGatewayV2::Integration	是	是
AWS::ApiGatewayV2::Stage	是	是
AWS::AppConfig::Application	是	是
AWS::AppConfig::ConfigurationProfile	是	是
AWS::AppConfig::DeploymentStrategy	是	是
AWS::AppConfig::Environment	是	是
AWS::AppConfig::Extension	是	是
AWS::AppConfig::ExtensionAssociation	是	是
AWS::AppConfig::HostedConfiguration版本	是	是
AWS::AppStream::AppBlock生成器	是	是
AWS::AppStream::Application	是	是
AWS::AppStream::DirectoryConfig	是	没有

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::AppStream::Fleet	是	没有
AWS::AppStream::Stack	是	没有
AWS::Athena::DataCatalog	是	是
AWS::Athena::WorkGroup	是	是
AWS::AutoScaling::AutoScaling组	是	是
AWS::AutoScaling::LaunchConfiguration	是	是
AWS::AutoScaling::ScalingPolicy	是	是
AWS::AutoScaling::ScheduledAction	是	是
AWS::AutoScaling::WarmPool	是	是
AWS::Backup::BackupPlan	是	是
AWS::Backup::BackupSelection	是	是
AWS::Backup::BackupVault	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::Backup::RecoveryPoint	是	是
AWS::BackupGateway::Hypervisor	是	是
AWS::Batch::ComputeEnvironment	是	是
AWS::Batch::JobQueue	是	是
AWS::Batch::SchedulingPolicy	是	是
AWS::Bedrock::Guardrail	是	是
AWS::Bedrock::KnowledgeBase	是	是
AWS::Bedrock::Prompt	是	是
AWS::Cassandra::Keyspace	是	是
AWS::CloudFormation::Stack	是	是
AWS::CloudFormation::StackSet	是	是
AWS::CloudTrail::EventData商店	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::CloudTrail::Trail	是	是
AWS::CloudWatch::Alarm	是	是
AWS::CodeBuild::Project	是	是
AWS::CodeBuild::ReportGroup	是	是
AWS::Cognito::IdentityPool	是	没有
AWS::Cognito::UserPool组	是	没有
AWS::Config::ConfigurationRecorder	是	是
AWS::Config::ConformancePack	是	是
AWS::Config::ConformancePack Compliance	是	是
AWS::Config::ResourceCompliance	是	是
AWS::Config::StoredQuery	是	是
AWS::Connect::Instance	是	没有

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::Connect::QuickConnect	是	没有
AWS::Connect::SecurityProfile	是	没有
AWS::Connect::User	是	没有
AWS::DMS::Certificate	是	是
AWS::DMS::Endpoint	是	是
AWS::DMS::EventSubscription	是	是
AWS::DMS::ReplicationInstance	是	是
AWS::DMS::ReplicationSubnet组	是	是
AWS::DMS::ReplicationTask	是	是
AWS::DataSync::Agent	是	是
AWS::DataSync::LocationEFS	是	是
AWS::DataSync::LocationFSxLustre	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::DataSync::LocationFSx窗户	是	是
AWS::DataSync::LocationHDFS	是	是
AWS::DataSync::LocationNFS	是	是
AWS::DataSync::LocationObject存储	是	是
AWS::DataSync::LocationS3	是	是
AWS::DataSync::Location中小型企业	是	是
AWS::DataSync::Task	是	是
AWS::Detective::Graph	是	是
AWS::DynamoDB::Table	是	是
AWS::EC2::CapacityReservation	是	是
AWS::EC2::ClientVpn端点	是	是
AWS::EC2::ClientVpnTargetNetworkAssociation	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::EC2::CustomerGateway	是	是
AWS:EC2::: DHCPOptions	是	是
AWS:EC2:: EC2 舰队	是	是
AWS:::EC2: EIP	是	是
AWS::EC2::EgressOnlyInternetGateway	是	是
AWS::EC2::FlowLog	是	是
AWS::EC2::Host	是	是
AWS:::EC2: IPAM	是	是
AWS:EC2::: IPAMPool	是	是
AWS::EC2:: IPAMPool Cidr	是	是
AWS::EC2: IPAMResource Discovery	是	是
AWS:EC2::: IPAMResource DiscoveryAssociation	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS:EC2::: IPAMScope	是	是
AWS::EC2::Instance	是	是
AWS::EC2::InstanceConnect端点	是	是
AWS::EC2::InternetGateway	是	是
AWS::EC2::LaunchTemplate	是	是
AWS::EC2::NatGateway	是	是
AWS::EC2::NetworkAcl	是	是
AWS::EC2::NetworkInterface	是	是
AWS::EC2::PrefixList	是	是
AWS::EC2::RouteTable	是	是
AWS::EC2::SecurityGroup	是	是
AWS::EC2::SecurityGroupVpcAssociation	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::EC2::SnapshotBlockPublicAccess	是	是
AWS::EC2::SpotFleet	是	是
AWS::EC2::Subnet	是	是
AWS::EC2::SubnetCidr屏蔽	是	是
AWS::EC2::SubnetNetworkAclAssociation	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是
AWS::EC2::TrafficMirror过滤器	是	是
AWS::EC2::TrafficMirrorSession	是	是
AWS::EC2::TrafficMirror目标	是	是
AWS::EC2::TransitGateway	是	没有
AWS::EC2::TransitGateway附件	是	是
AWS::EC2::TransitGatewayConnect	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::EC2::TransitGatewayMulticastDomain	是	是
AWS::EC2::TransitGatewayRouteTable	是	是
AWS:::EC2: VPC	是	是
AWS:EC2::: VPCBlock PublicAccessExclusion	是	是
AWS:EC2::: VPCBlock PublicAccessOptions	是	是
AWS:EC2::: VPCEndpoint	是	是
AWS:EC2::: VPCEndpoint ConnectionNotification	是	是
AWS:EC2::: VPCEndpoint 服务	是	没有
AWS::EC2:: VPCGateway 附件	是	是
AWS:EC2:: VPCPeering 连接	是	是
AWS:EC2::: VPNConnection	是	是
AWS::EC2:: VPNConnection 路线	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS:EC2::: VPNGateway	是	是
AWS::EC2::VerifiedAccess实例	是	是
AWS::EC2::Volume	是	是
AWS::ECR::ReplicationConfiguration	是	是
AWS::ECR::Repository	是	是
AWS::ECS::CapacityProvider	是	是
AWS::ECS::Cluster	是	是
AWS::ECS::Service	是	是
AWS::ECS::TaskDefinition	是	是
AWS::ECS::TaskSet	是	是
AWS::EFS::AccessPoint	是	是
AWS::EFS::FileSystem	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::EKS::Addon	是	是
AWS::EKS::Cluster	是	是
AWS::EKS::IdentityProviderConfig	是	是
AWS::EMR::SecurityConfiguration	是	是
AWS::EMR::Studio	是	是
AWS::EMRContainers::VirtualCluster	是	是
AWS::ElasticBeanstalk::Application	是	是
AWS::ElasticBeanstalk::ApplicationVersion	是	是
AWS::ElasticBeanstalk::Environment	是	是
AWS::ElasticLoadBalancing::LoadBalancer	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::ElasticLoadBalancingV2::TargetGroup	是	是
AWS::Elasticsearch::Domain	是	是
AWS::Events::EventBus	是	是
AWS::Events::Rule	是	是
AWS::FIS::ExperimentTemplate	是	是
AWS::Glue::Classifier	是	是
AWS::Glue::Job	是	是
AWS::Glue::MLTransform	是	没有
AWS::Glue::Registry	是	是
AWS::GreengrassV2::ComponentVersion	是	是
AWS::GuardDuty::Detector	是	是
AWS::GuardDuty::Filter	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::Guard职责:: IPSet	是	是
AWS::GuardDuty::ThreatIntel设置	是	是
AWS::IAM::Group	是	是
AWS::IAM::InstanceProfile	没有	是
AWS:: IAM:: OIDCProvider	没有	是
AWS::IAM::Policy	是	是
AWS::IAM::Role	是	是
AWS:: IAM:: SAMLProvider	没有	是
AWS::IAM::ServerCertificate	没有	是
AWS::IAM::User	是	是
AWS::ImageBuilder::ContainerRecipe	是	是
AWS::ImageBuilder::DistributionConfiguration	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::ImageBuilder::ImagePipeline	是	是
AWS::ImageBuilder::ImageRecipe	是	是
AWS::ImageBuilder::InfrastructureConfiguration	是	是
AWS::InspectorV2::Activation	是	是
AWS::IoT::AccountAudit配置	是	是
AWS::IoT::Authorizer	是	是
AWS::IoT:: CACertificate	是	是
AWS::IoT::CustomMetric	是	是
AWS::IoT::Dimension	是	是
AWS::IoT::FleetMetric	是	是
AWS::IoT::JobTemplate	是	是
AWS::IoT::MitigationAction	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::IoT::Policy	是	是
AWS::IoT::ProvisioningTemplate	是	是
AWS::IoT::RoleAlias	是	是
AWS::IoT::ScheduledAudit	是	是
AWS::IoT::SecurityProfile	是	是
AWS::IoT::ThingGroup	是	是
AWS::IoTEvents::AlarmModel	是	没有
AWS::IoTEvents::DetectorModel	是	没有
AWS::IoTEvents::Input	是	没有
AWS::IoTSiteWise::Asset	是	没有
AWS::IoTSiteWise::AssetModel	是	没有
AWS::IoTSiteWise::Gateway	是	没有

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::IoTSiteWise::Portal	是	没有
AWS::IoTTwinMaker::ComponentType	是	没有
AWS::IoTTwinMaker::Entity	是	没有
AWS::IoTTwinMaker::Workspace	是	没有
AWS::KMS::Alias	是	是
AWS::KMS::Key	是	是
AWS::Kinesis::Stream	是	是
AWS::Kinesis::StreamConsumer	是	是
AWS::KinesisAnalyticsV2::Application	是	是
AWS::KinesisFirehose::DeliveryStream	是	是
AWS::Lambda::Function	是	是
AWS::Location::GeofenceCollection	是	没有

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::Location::Map	是	没有
AWS::Location::PlaceIndex	是	没有
AWS::Location::RouteCalculator	是	没有
AWS::Logs::Destination	是	是
AWS::MSK::BatchScram秘密	是	是
AWS::MSK::Cluster	是	是
AWS::MSK::ClusterPolicy	是	是
AWS::MSK::Configuration	是	是
AWS::MSK::VpcConnection	是	是
AWS::NetworkFirewall::Firewall	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是
AWS::NetworkFirewall::RuleGroup	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::NetworkFirewall::VpcEndpoint协会	是	是
AWS::NetworkManager::CustomerGateway协会	是	没有
AWS::NetworkManager::Device	是	没有
AWS::NetworkManager::GlobalNetwork	是	没有
AWS::NetworkManager::Link	是	没有
AWS::NetworkManager::LinkAssociation	是	没有
AWS::NetworkManager::Site	是	没有
AWS::NetworkManager::TransitGateway注册	是	没有
AWS::OpenSearch::Domain	是	是
AWS::OpenSearchServerless::SecurityConfig	是	是
AWS::Pinpoint::App	是	没有
AWS::Pinpoint::ApplicationSettings	是	没有

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::Pinpoint::Campaign	是	没有
AWS::Pinpoint::EmailChannel	是	没有
AWS::Pinpoint::EmailTemplate	是	没有
AWS::Pinpoint::EventStream	是	没有
AWS::Pinpoint::InApp模板	是	没有
AWS::Pinpoint::Segment	是	没有
AWS::QuickSight::Dashboard	是	是
AWS::QuickSight::Template	是	没有
AWS:: RDS:: DBCluster	是	是
AWS:: RDS:: 快照 DBCluster	是	是
AWS:: RDS:: DBInstance	是	是
AWS:: RDS:: 终端节点 DBProxy	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS:: RDS:: 群组 DBSecurity	是	是
AWS:: RDS:: DBSnapshot	是	是
AWS:: RDS:: 群组 DBSubnet	是	是
AWS::RDS::EventSubscription	是	是
AWS::RDS::OptionGroup	是	是
AWS::Redshift::Cluster	是	是
AWS::Redshift::ClusterParameter组	是	是
AWS::Redshift::ClusterSecurity组	是	是
AWS::Redshift::ClusterSnapshot	是	是
AWS::Redshift::ClusterSubnet组	是	是
AWS::Redshift::EventSubscription	是	是
AWS::Redshift::Integration	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::Redshift::ScheduledAction	是	是
AWS::RoboMaker::RobotApplication	是	没有
AWS::RoboMaker::RobotApplication版本	是	没有
AWS::RoboMaker::SimulationApplication	是	没有
AWS::Roles任何地方:: CRL	是	是
AWS::RolesAnywhere::Profile	是	是
AWS::RolesAnywhere::TrustAnchor	是	是
AWS::Route53Profiles::Profile	是	是
AWS::Route53Profiles::ProfileAssociation	是	是
AWS::Route53Resolver::FirewallDomain清单	是	是
AWS::Route53Resolver::FirewallRule组	是	是
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::Route53Resolver::ResolverEndpoint	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	是	是
AWS::Route53Resolver::ResolverRule	是	是
AWS::Route53Resolver::ResolverRule协会	是	是
AWS::S3::AccessGrant	是	是
AWS::S3::AccessGrants实例	是	是
AWS::S3::AccessGrantsLocation	是	是
AWS::S3::AccessPoint	是	是
AWS::S3::AccountPublicAccessBlock	是	是
AWS::S3::Bucket	是	是
AWS::SES::ConfigurationSet	是	没有

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::SES::ContactList	是	没有
AWS::SES::DedicatedIp泳池	是	是
AWS::SES::Template	是	没有
AWS::SNS::Topic	是	是
AWS::SQS::Queue	是	是
AWS::SSM::AssociationCompliance	是	是
AWS::SSM::Document	是	是
AWS::SSM::FileData	是	是
AWS::SSM::ManagedInstance 清单	是	是
AWS::SSM::PatchCompliance	是	是
AWS::SSM::ResourceData同步	是	是
AWS::SageMaker::Model	是	没有

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::SageMaker::NotebookInstance	是	没有
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	没有
AWS::SageMaker::StudioLifecycleConfig	是	是
AWS::SageMaker::UserProfile	是	是
AWS::SecretsManager::ResourcePolicy	是	是
AWS::SecretsManager::RotationSchedule	是	是
AWS::SecretsManager::Secret	是	是
AWS::SecurityHub::Standard	是	是
AWS::ServiceCatalog::CloudFormation产品	是	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是
AWS::ServiceCatalog::Portfolio	是	是
AWS::ServiceDiscovery::HttpNamespace	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::ServiceDiscovery::Instance	是	是
AWS::ServiceDiscovery::Service	是	是
AWS::StepFunctions::StateMachine	是	是
AWS::Transfer::Agreement	是	是
AWS::Transfer::Certificate	是	是
AWS::Transfer::Connector	是	是
AWS::Transfer::Profile	是	是
AWS::Transfer::Server	是	是
AWS::Transfer::Workflow	是	是
AWS::WAFRegional::RateBased规则	是	是
AWS::WAFRegional::Rule	是	是
AWS::WAFRegional::RuleGroup	是	是

资源类型	Amazon GovCloud（美国西部）	Amazon GovCloud（美国东部）
AWS::WAFRegional::WebACL	是	是
AWS:WAFv2::: IPSet	是	是
AWS::WAFv2::ManagedRule设置	是	是
AWS::WAFv2::RegexPattern设置	是	是
AWS::WAFv2::RuleGroup	是	是
AWS::WAFv2::WebACL	是	是
AWS::WorkSpaces::Workspace	是	没有

使用 Amazon Config 记录 Amazon 资源

Amazon Config 将持续检测受支持资源类型的创建、更改或删除时间。Amazon Config 会将这些事件记录为配置项（CI）。

您可以自定义，Amazon Config以使其记录所有受支持类型的资源的配置更改，或仅记录与您相关的资源类型的配置更改。有关 Amazon Config 可以记录的受支持资源类型的列表，请参阅 支持的资源类型 Amazon Config

主题

- 注意事项
- 区域性资源和全局资源有什么区别？
- Amazon Config 规则和全局资源类型

- Amazon Config 记录频率
- 未记录的资源
- 在 Amazon Config 控制台中记录资源
- 使用 Amazon CLI 记录资源
- 从 Amazon Config 记录中排除资源
- 停止 Amazon Config 使用客户管理的配置记录器进行记录

注意事项

大量 Amazon Config 评估

您可能会注意到，在最初使用 Amazon Config 记录的一个月中，账户活动会多于随后的几个月。在初始引导过程中，Amazon Config 会对您账户中选择的、需要 Amazon Config 记录的所有资源进行评估。

如果您运行的是临时工作负载，则可能会看到 Amazon Config 中的活动增加，因为它会记录与创建和删除这些临时资源相关的配置更改。临时工作负载 是临时使用在需要时加载和运行的计算资源。示例包括 Amazon Elastic Compute Cloud（Amazon EC2）竞价型实例、Amazon EMR 任务和 Amazon Auto Scaling。

如果您想避免因运行临时工作负载而导致活动增加，则可以设置客户管理的配置记录器，将这些资源类型排除在记录范围之外，或者在单独的账户中运行这些类型的工作负载，同时将 Amazon Config 关闭，以避免增加配置记录和规则评估。

区域可用性

在指定 Amazon Config 要跟踪的资源类型之前，请检查按区域可用性列出的资源覆盖范围，以查看您设置 Amazon Config 的 Amazon 区域是否支持该资源类型。

如果 Amazon Config 至少在一个区域支持某种资源类型，则即使您设置 Amazon Config 的 Amazon 区域不支持指定的资源类型，您也可以在 Amazon Config 支持的所有区域中启用该资源类型的记录。

区域性资源和全局资源有什么区别？

区域性资源

区域性资源与某个区域相关联，且仅可在该区域中使用。您在指定 Amazon Web Services 区域中创建它们，然后它们就存在于该区域中。要查看这些资源或与之交互，您必须将操作

定向到该区域。例如，要使用 Amazon Web Services 管理控制台创建 Amazon EC2 实例 Amazon Web Services 区域，应选择要在中创建实例的。如果您使用 Amazon Command Line Interface（Amazon CLI）创建实例，则需要包含 `--region` 参数。每个 Amazon SDK 都有自己的等效机制来指定操作所用的区域。

使用区域性资源有几个原因。原因之一是要确保资源以及您用来访问资源的服务终端节点尽可能靠近客户。这通过最大限度减少延迟来提高性能。另一个原因是为了提供隔离边界。这样，您可以在多个区域中创建独立的资源副本，以分配负载并提高可扩展性。同时，它可以将资源相互隔离，以提高可用性。

如果您在控制台或 Amazon CLI 命令中指定不同的，Amazon Web Services 区域则无法再查看在前一个区域中可以看到的资源或与之交互。

当您查看区域资源的 Amazon 资源名称（ARN）时，包含该资源的区域被指定为 ARN 中的第四个字段。例如，Amazon EC2 实例是一种区域性资源。以下是面向 `us-east-1` 区域中 Amazon EC2 实例的 ARN 示例。

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

全局资源

有些 Amazon 服务资源是全局资源，这意味着您可以从任何地方 使用该资源。您无需在全局服务的控制台中指定。Amazon Web Services 区域要访问全局资源，在使用服务的 Amazon CLI 和 Amazon SDK 操作时请勿指定 `--region` 参数。

全局资源支持在关键时刻某一特定资源只能存在一个实例的情况。在这些情况下，在不同区域的副本之间进行复制或同步是不够的。为了确保资源使用者能即时看到任何变化，访问单一全局终端节点被认为是可以接受的，虽然可能会增加延迟。

例如，Amazon Aurora 全局集群（`AWS::RDS::GlobalCluster`）是全局资源，因此与区域无关。这意味着您无需依赖区域终端节点即可创建全局集群。好处是，虽然 Amazon Relational Database Service（Amazon RDS）本身是按区域组织的，但全局集群所源自的特定区域不会影响全局集群。它以单个连续的全局集群形式出现在所有区域。

全局资源的 Amazon 资源名称（ARN）不包括区域。第四个字段为空，例如以下全局集群的 ARN 示例。

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> 2022 年 2 月之后载入 Amazon Config 的全局资源类型将仅在服务的主区域中（对于商业分区）和 Amazon GovCloud（美国西部）中（对于 GovCloud 分区）进行记录。您只能在主区域和 Amazon GovCloud（美国西部）查看这些新全局资源类型的配置项（CI）。
> 2022 年 2 月之前载入的全局资源类型（`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role` 和 `AWS::IAM::User`）保持不变。您可以在 2022 年 2 月之前支持 Amazon Config 的所有区域启用这些全局 IAM 资源的记录。在 2022 年 2 月之后支持 Amazon Config 的区域中，无法记录这些全局 IAM 资源。

全局资源类型 | IAM 资源

以下 IAM 资源类型是全局资源：IAM 用户、组、角色和客户管理型策略。这些资源类型可以在 2022 年 2 月之前 Amazon Config 可用的区域中由 Amazon Config 进行记录。无法记录全局 IAM 资源类型的区域列表中包含以下区域：亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、亚太地区（泰国）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）、以色列（特拉维夫）、墨西哥（中部）和中东（阿联酋）。

为避免配置项（CI）重复，您应考虑仅在一个支持的区域内记录全局 IAM 资源类型。这还可以帮助您避免不必要的评估和 API 节流。

全局资源类型 | 仅限主区域

以下服务的全局资源仅由 Amazon Config 记录在全局资源类型的主区域中：Amazon Elastic Container Registry Public、Amazon Global Accelerator、Amazon Route 53、Amazon CloudFront 和 Amazon WAF。对于这些全局资源，可以在多个 Amazon 区域中使用资源类型的相同实例，但是配置项（CI）仅记录在商业分区的主区域或 Amazon GovCloud (US) 分区的 Amazon GovCloud（美国西部）区域。

全局资源类型的主区域

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

Amazon 服务	资源类型值	主区域
	AWS::GlobalAccelerator::EndpointGroup	美国西部（俄勒冈州）区域
	AWS::GlobalAccelerator::Accelerator	美国西部（俄勒冈州）区域
Amazon Route 53	AWS::Route53::HostedZone	美国东部（弗吉尼亚州北部）区域
	AWS::Route53::HealthCheck	美国东部（弗吉尼亚州北部）区域
Amazon CloudFront	AWS::CloudFront::Distribution	美国东部（弗吉尼亚州北部）区域
Amazon WAF	AWS::WAFv2::WebACL	美国东部（弗吉尼亚州北部）区域

全局资源类型 | Aurora 全局集群

AWS::RDS::GlobalCluster 是一种全局资源，记录在所有已启用客户管理的配置记录器的受支持 Amazon Config 区域中。这种全局资源类型的独特之处在于，如果您在一个区域中启用对此资源的记录，Amazon Config 将在所有已启用的区域中记录该资源类型的配置项（CI）。

如果您不想在所有已启用的区域中记录，AWS::RDS::GlobalCluster请使用以下适用于 Amazon Config 控制台的记录策略之一：

- 记录所有资源类型，并使用可自定义的覆盖，选择“Amazon RDS GlobalCluster”，然后选择“从记录中排除”覆盖方法
- 记录特定的资源类型（ ）。

如果您不想在所有已启用的区域中记录，AWS::RDS::GlobalCluster请使用以下适用于 API/CLI 的记录策略之一：

- 记录所有当前和未来的资源类型，排除项除外（EXCLUSION_BY_RESOURCE_TYPES）
- 记录特定的资源类型（INCLUSION_BY_RESOURCE_TYPES）。

Amazon Config 规则和全局资源类型

2022 年 2 月之前载入的全局 IAM 资源类型（`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role` 和 `AWS::IAM::User`）只能由 Amazon Config 在 2022 年 2 月之前 Amazon Config 已可用的区域中进行记录。在 2022 年 2 月之后支持 Amazon Config 的区域中，无法记录这些全局 IAM 资源类型。有关这些区域的列表，请参阅记录 Amazon 资源 | 全球资源。

如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。

在 2022 年 2 月之前报告载入的全局资源的最佳实践

为避免不必要的评估，您只能在支持的某个区域中部署具有这些全局资源的 Amazon Config 规则和合规包。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。这适用于 Amazon Config 规则、组织 Amazon Config 规则以及由其他 Amazon 服务（例如 Amazon Security Hub CSPM 和 Amazon Control Tower）创建的规则。

如果您没有记录 2022 年 2 月之前载入的全局资源类型，建议您不要启用以下定期规则，以避免不必要的评估：

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled
- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

在 2022 年 2 月之后报告载入的全局资源的最佳实践

2022 年 2 月之后载入 Amazon Config 记录的全局资源类型，将仅在服务的主区域中（对于商业分区）和 Amazon GovCloud（美国西部）中（对于 Amazon GovCloud (US) 分区）进行记录。您应仅在资源

类型的主区域中部署具有这些范围内全局资源的 Amazon Config 规则和合规性包。有关更多信息，请参阅全局资源类型的主区域。

Amazon Config 记录频率

Amazon Config 支持连续记录 和每日记录。连续记录可让您在每次发生配置更改时连续记录更改。使用每日记录，您将收到代表过去 24 小时内资源的最新状态的配置项（CI），前提是它与之前记录的 CI 不同。有关如何更改录制频率的步骤，请参阅更改录制频率。

连续记录

连续记录的部分优势包括：

- 实时监控：连续记录可以立即检测未经授权的更改或意外改动，从而提升您的安全性和合规性。
- 详细分析：连续记录可以让您在资源配置更改发生时对其进行深入分析，确定当下的模式和趋势。

每日记录

每日记录的部分优势包括：

- 最大限度减少干扰：每日记录可以为您提供更易于管理的信息流，从而减少通知频率和警报疲劳。
- 成本效益：每日记录可以让您灵活地以较低的频率记录资源更改，从而降低与记录的配置更改数量相关的成本。

> **Note**
>
> Amazon Firewall Manager 依赖连续记录来监控您的资源。如果您使用的是 Firewall Manager，建议您将记录频率设置为“持续”。

未记录的资源

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

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

IAM 资源类型注意事项

仅当资源被选为或以前被选为要在客户管理的配置记录器中记录的资源时，AWS::IAM::User、AWS::IAM::Policy、 AWS::IAM::Group、AWS::IAM::Role 资源类型才会捕获创建（ResourceNotRecorded）和删除（ResourceDeletedNotRecorded）状态。

未记录资源的 CI 记录时间表

ResourceNotRecorded 和 ResourceDeletedNotRecorded 的配置项目（CI）不遵循资源类型的典型录制时间。这些资源类型仅在客户管理的配置记录器的定期基准化过程中进行记录，与其他资源类型相比，该过程的频率较低。这意味着创建和删除通知不是在创建或删除时发送的，而是在基准化过程中发送的。

CI 交付和服务相关记录器范围

对于服务相关配置记录器，记录范围决定您是否在传送通道中收到配置项（CI）。记录范围由关联到配置记录器的服务设置。如果记录范围是内部，则您不会在传输通道中收到 CI。

在 Amazon Config 控制台中记录资源

您可以使用 Amazon Config 控制台选择 Amazon Config 要通过客户管理的配置记录器进行记录的资源类型。

选择资源

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在左侧导航窗格中，选择设置。
3. 在客户管理的记录器选项卡上，选择编辑。
4. 在记录方法部分，选择记录策略。指定您希望 Amazon Config 记录的 Amazon 资源。

   All resource types with customizable overrides

   设置，Amazon Config以记录该区域中所有当前和未来支持的资源类型的配置更改。您可以覆盖特定资源类型的记录频率，也可以从记录中排除特定资源类型。有关更多信息，请参阅支持的资源类型。

   - 默认设置

     为所有当前和未来支持的资源类型配置默认记录频率。有关更多信息，请参阅记录频率。

     - 连续记录 - Amazon Config 在发生更改时连续记录配置更改。

- 每日记录 - 您会收到代表过去 24 小时内资源的最新状态的配置项（CI），前提是它与之前记录的 CI 不同。

> **Note**
>
> Amazon Firewall Manager 依赖连续记录来监控您的资源。如果您使用的是 Firewall Manager，建议您将记录频率设置为“持续”。

- 覆盖设置

覆盖特定资源类型的记录频率，或从记录中排除特定资源类型。如果您更改某一资源类型的记录频率或停止记录某一资源类型，则已记录的配置项会保持不变。

Specific resource types

设置，Amazon Config以仅记录您指定的资源类型的配置更改。

- 特定的资源类型

选择要记录的资源类型及其频率。有关更多信息，请参阅记录频率。

- 连续记录 - Amazon Config 在发生更改时连续记录配置更改。
- 每日记录 - 您会收到代表过去 24 小时内资源的最新状态的配置项（CI），前提是它与之前记录的 CI 不同。

> **Note**
>
> Amazon Firewall Manager 依赖连续记录来监控您的资源。如果您使用的是 Firewall Manager，建议您将记录频率设置为“持续”。

如果您更改某一资源类型的记录频率或停止记录某一资源类型，则已记录的配置项会保持不变。

5. 选择 保存 以保存您的更改。

记录资源时的注意事项

大量 Amazon Config 评估

您可能会注意到，在最初使用 Amazon Config 记录的一个月中，账户活动会多于随后的几个月。在初始引导过程中，Amazon Config 会对您账户中选择的、需要 Amazon Config 记录的所有资源进行评估。

如果您运行的是临时工作负载，则可能会看到 Amazon Config 中的活动增加，因为它会记录与创建和删除这些临时资源相关的配置更改。临时工作负载 是临时使用在需要时加载和运行的计算资源。示例包括 Amazon Elastic Compute Cloud（Amazon EC2）竞价型实例、Amazon EMR 任务和 Amazon Auto Scaling。如果您想避免因运行临时工作负载而导致活动增加，则可以设置客户管理的配置记录器，将这些资源类型排除在记录范围之外，或者在单独的账户中运行这些类型的工作负载，同时将 Amazon Config 关闭，以避免增加配置记录和规则评估。

Considerations: All resource types with customizable overrides

全局记录的资源类型 | Aurora 全局集群最初包含在记录范围内

`AWS::RDS::GlobalCluster` 资源类型将记录在已启用客户管理的配置记录器的所有受支持 Amazon Config 区域中。

如果您不想在所有已启用的区域中记录，`AWS::RDS::GlobalCluster`请选择“Amazon RDS GlobalCluster”，然后选择“从记录中排除”覆盖方法。

全局资源类型 | IAM 资源类型最初不包含在记录范围内

为了帮您降低成本，全局 IAM 资源类型最初将不包含在记录范围内。此捆绑包包括 IAM 用户、组、角色和客户管理型策略。选择移除以删除覆盖，并将这些资源包含在您的记录范围内。

此外，Amazon Config 在 2022 年 2 月之后提供支持的区域中，无法记录以下全局 IAM 资源类型：`AWS::IAM::User`、`AWS::IAM::Group`、`AWS::IAM::Role` 和 `AWS::IAM::Policy`。有关这些区域的列表，请参阅记录 Amazon 资源 | 全球资源。

限制

您可以添加最多 100 项频率覆盖和 600 项排除覆盖。

以下资源类型不支持每日记录：

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

Considerations: Specific resource types

区域可用性

在指定 Amazon Config 要跟踪的资源类型之前，请检查按区域可用性列出的资源覆盖范围，以查看您设置 Amazon Config 的 Amazon 区域是否支持该资源类型。如果 Amazon Config 至少在一个区域支持某种资源类型，则即使您设置 Amazon Config 的 Amazon 区域不支持指定的资源类型，您也可以在 Amazon Config 支持的所有区域中启用该资源类型的记录。

限制

如果所有资源类型的频率都相同，则没有限制。如果至少将一种资源类型设置为“持续”，则最多可以添加 100 种频率为“每日”的资源类型。

以下资源类型不支持“每日”频率：

- `AWS::Config::ResourceCompliance`
- `AWS::Config::ConformancePackCompliance`
- `AWS::Config::ConfigurationRecorder`

使用 Amazon CLI 记录资源

您可以使用 Amazon CLI 选择您希望 Amazon Config 记录的资源类型。为此，您可以创建一个客户管理的配置记录器，以记录您在记录组中指定的资源类型。在记录组中，您可以指定是要记录所有受支持的资源类型，还是包括或排除特定类型的资源。

Record all current and future supported resource types

设置，Amazon Config以记录该区域中所有当前和未来支持的资源类型的配置更改。有关支持的资源类型列表，请参阅支持的资源类型。

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

   此命令使用 `--configuration-recorder` 和 `---recording-group` 字段。

   ```
   $ aws configservice put-configuration-recorder \
   --configuration-recorder file://configurationRecorder.json \
   --recording-group file://recordingGroup.json
   ```

   `configuration-recorder` 字段

configurationRecorder.json 文件指定配置记录器的 name 和 roleArn 以及默认记录频率（recordingMode）。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

recording-group 字段

recordingGroup.json 文件指定要记录哪些资源类型。

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

有关这些字段的更多信息，请参阅《Amazon CLI 命令参考》中的 put-configuration-recorder

2. （可选）要验证您的客户管理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": [
        {
            "name": "default"
            "recordingGroup": {
                "allSupported": true,
                "exclusionByResourceTypes": {
                     "resourceTypes": []
                },
                "includeGlobalResourceTypes": true,
                "recordingStrategy": {
                    "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types
 to include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record all current and future supported resources types excluding the types you specify

设置，Amazon Config以记录包括全局资源类型在内的所有当前和未来支持的资源类型的配置更改，但您指定要从记录中排除的资源类型除外。

如果您选择停止记录某一资源类型，则已记录的配置项将保持不变。有关支持的资源类型列表，请参阅支持的资源类型。

1. 使用 put-configuration-recorder 命令：

此命令使用 --configuration-recorder 和 ---recording-group 字段。

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

configuration-recorder 字段

configurationRecorder.json 文件指定配置记录器的 name 和 roleArn 以及默认记录频率（recordingMode）。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

recording-group 字段

recordingGroup.json 文件指定 Amazon Config 将记录的资源类型。在 exclusionByResourceTypes 的 resourceTypes 字段中传递一个或多个要排除的资源类型，如以下示例所示。

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
```

```
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

有关这些字段的更多信息，请参阅《Amazon CLI 命令参考》中的 [put-configuration-recorder]

2. （可选）要验证您的客户管理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": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
                "recordingStrategy": {
                    "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [],
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
```

```
                    "description": "Description you provide for the override,
                    "recordingFrequency": CONTINUOUS or DAILY,
                    "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

Record specific resource types

设置，Amazon Config以仅记录您指定的资源类型的配置更改。

如果您选择停止记录某一资源类型，则已记录的配置项将保持不变。有关支持的资源类型列表，请参阅[支持的资源类型]。

1. 使用 [put-configuration-recorder] 命令：

   此命令使用 --configuration-recorder 和 ---recording-group 字段。

```
$ aws configservice put-configuration-recorder \
--configuration-recorder file://configurationRecorder.json \
--recording-group file://recordingGroup.json
```

   configuration-recorder 字段

   configurationRecorder.json 文件指定配置记录器的 name 和 roleArn 以及默认记录频率（recordingMode）。

```
{
  "name": "default",
  "roleARN": "arn:aws:iam::123456789012:role/config-role",
  "recordingMode": {
    "recordingFrequency": CONTINUOUS or DAILY,
    "recordingModeOverrides": [
        {
            "description": "Description you provide for the override",
            "recordingFrequency": CONTINUOUS or DAILY,
```

```
            "resourceTypes": [ Comma-separated list of resource types to include
 in the override ]
        }
    ]
  }
}
```

recording-group 字段

recordingGroup.json 文件指定 Amazon Config 将记录的资源类型。在 resourceTypes 字段中传递一个或多个要排除的资源类型，如以下示例所示。

```
{
    "allSupported": false,
    "recordingStrategy": {
        "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
    },
    "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"
  ]
}
```

有关这些字段的更多信息，请参阅《Amazon CLI 命令参考》中的 put-configuration-recorder

2. （可选）要验证您的客户管理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": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "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"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

从 Amazon Config 记录中排除资源

Amazon Config 允许您将特定类型的 Amazon 资源排除在清单跟踪和合规性监控之外，同时仍可以跟踪 Amazon Config 中当前可用的所有其他受支持的资源类型，包括以后要添加的资源类型。您可以使用此功能将注意力集中在受合规性和监管标准约束的关键资源上。

Excluding resources (Console)

如果您不想记录 Amazon 资源类型，请使用以下适用于 Amazon Config 控制台的记录策略之一：

- 记录所有资源类型，并使用可自定义的覆盖，选择要排除的资源类型，然后选择“从记录中排除”覆盖方法
- 记录特定的资源类型（ ）。

有关更多详细步骤，请参阅记录资源（控制台）。

Excluding resources (Amazon CLI)

如果您不想记录 Amazon 资源类型，请使用以下适用于 API/CLI 的记录策略之一：

- 记录所有当前和未来的资源类型，排除项除外（`EXCLUSION_BY_RESOURCE_TYPES`）
- 记录特定的资源类型（`INCLUSION_BY_RESOURCE_TYPES`）。

有关更多详细步骤，请参阅录制资源（Amazon CLI）。

停止 Amazon Config 使用客户管理的配置记录器进行记录

您可以随时停止 Amazon Config 使用客户管理的配置记录器进行录制。在 Amazon Config 停止记录某个资源后，它会保留之前捕获的配置信息，并且您可继续访问此类信息。

有关如何停止记录的步骤，请参阅停止客户管理的配置记录器。

使用 Amazon CLI 记录 Amazon Config 第三方资源的配置

记录第三方资源或自定义资源类型的配置，例如本地服务器、SaaS 监控工具和版本控制系统（例如 GitHub）上的配置。

您可以使用 Amazon Config 控制台和 API，将第三方资源的配置数据发布到 Amazon Config 中并查看和监控资源清单及配置历史记录。您可以使用 Amazon Config 管理所有资源，并使用 Amazon Config

规则评估资源配置是否符合最佳实践。您还可以创建 Amazon Config 规则或合规包，以根据最佳实践、内部策略和监管策略评估这些第三方资源。

> **Note**
>
> 如果您已将 Amazon Config 配置为记录所有资源类型，则系统会自动在 Amazon Config 中将通过 Amazon CloudFormation 管理（创建、更新或删除）的第三方资源作为配置项目进行跟踪。

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

主题

- 将第三方资源添加到 Amazon Config
- 使用 Amazon CLI 记录 Amazon Config 第三方资源的配置项
- 使用 Amazon CLI 读取 Amazon Config 第三方资源的配置项
- 使用 Amazon CLI 从 Amazon Config 删除第三方资源

将第三方资源添加到 Amazon Config

按照以下步骤向 Amazon Config 中添加第三方资源。

主题

- 步骤 1：设置开发环境
- 步骤 2：资源建模
- 步骤 3：生成构件
- 步骤 4：注册资源
- 步骤 5：发布资源配置

步骤 1：设置开发环境

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

步骤 2：资源建模

创建符合资源类型配置的资源提供程序架构，并验证该架构。

1. 使用 `init` 命令创建资源提供程序项目并生成所需的文件。

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

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

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

3. 输入资源的包名称。

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

> **Note**
>
> 为了确保正确解析任何项目依赖关系，您可以将生成的项目导入支持 Maven 的 IDE 中。例如，如果您使用的是 IntelliJ IDEA，则需要执行以下操作：
>
> - 从文件菜单中，选择新建，然后选择现有源中的项目。
> - 导航到项目目录。
> - 在导入项目对话框中，选择从外部模型导入项目，然后选择 Maven。
> - 选择下一步，并接受所有默认设置以完成项目导入。

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

```
{
  "typeName": "MyCustomNamespace::Testing::WordPress",
  "description": "An example resource that creates a website based on WordPress
 5.2.2.",
  "properties": {
    "Name": {
```

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

5. 验证架构。

```
$ cfn validate
```

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

```
$ cfn generate
```

> **Note**
>
> 使用 Maven 时，作为编译过程的一部分，`generate` 命令会在编译代码之前自动运行。因此，您的更改永远不会与生成的代码不同步。
> 请注意，CloudFormation CLI 必须位于 Maven/系统可以找到的位置。有关更多信息，请参阅设置用于开发扩展的环境。

有关整个过程的更多信息，请参阅对资源提供程序进行建模以在 Amazon CloudFormation 中使用。

步骤 3：生成构件

运行以下命令以生成 `cfn submit` 的构件。

```
$ mvn package
```

步骤 4：注册资源

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

```
$ cfn submit
```

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

步骤 5：发布资源配置

确定 MyCustomNamespace::Testing::WordPress 的配置。

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

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

在 Amazon Config 中，可以查看是否接受了此资源配置。要评估合规性，您可以编写使用此资源的 Amazon Config 规则。

（可选）要自动记录配置，请实施定期配置收集器或基于更改的配置收集器。

使用 Amazon CLI 记录 Amazon Config 第三方资源的配置项

使用以下过程记录第三方资源或自定义资源类型的配置项：

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

1. 打开命令提示符或终端窗口。
2. 输入以下命令：

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> 按照类型架构中的定义，将在 Amazon Config 记录之前从配置中删除。`writeOnlyProperties`这意味着，当通过读取 API 获取配置时，这些值将不存在。有关 `writeOnlyProperties` 的更多信息，请参阅资源类型架构。

使用 Amazon CLI 读取 Amazon Config 第三方资源的配置项

使用以下过程读取第三方资源或自定义资源类型的配置项：

1. 打开命令提示符或终端窗口。
2. 输入以下命令：

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

3. 按 Enter。

   您应该可以看到类似于如下所示的输出内容：

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

```
}
```

4. 输入以下命令：

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

5. 按 Enter。

   您应该可以看到类似于如下所示的输出内容：

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

使用 Amazon CLI 从 Amazon Config 删除第三方资源

输入以下命令以删除第三方资源：

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

如果成功，则命令会执行，而没有附加输出。

使用 Amazon Config 记录托管实例的软件配置

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

主题

- 先决条件
- 记录软件配置

先决条件

您必须完成以下步骤来记录软件配置变更：

- 在 Amazon Config 中打开对托管实例清单资源类型的记录。
- 将 EC2 和本地服务器配置为 Amazon Systems Manager 中的托管实例。托管实例是一台已配置为与 Systems Manager 一起使用的计算机。
- 使用 Systems Manager 清单功能启动收集托管实例的软件清单。

> **Note**
>
> Systems Manager 现在支持为非托管实例创建配置项
> 非托管实例的配置项将拥有具有 `Key: “InstanceStatus”` 和 `Value: “Unmanaged”` 的补充配置。
> 非托管实例的配置项不会接收其他更新
> 要接收其他更新，配置项必须是托管实例。

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

记录软件配置

在 Amazon Config 中启用软件配置变更的记录：

1. 在 Amazon Config 中记录所有支持的资源类型，或选择性地记录托管实例清单资源类型。有关更多信息，请参阅 使用 Amazon Config 记录 Amazon 资源
2. 启动带有 Systems Manager 实例配置文件的 Amazon EC2 实例，该配置文件中包含 AmazonSSMManagedInstanceCore 托管策略。此 Amazon 托管策略使实例能够使用 Systems Manager 服务核心功能。

   有关可以添加到 Systems Manager 的实例配置文件中的其他策略的信息，请参阅《Amazon Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

   > **Important**
   >
   > SSM 代理是必须安装在托管实例上的 Amazon 软件，以便在云中与 Systems Manager 进行通信。如果您的 EC2 实例是从 AMI 为以下一种操作系统创建的，则会预装代理：
   >
   > - 2016 年 11 月或之后发布的 Windows Server 2003-2012 R2 AMI
   > - Windows Server 2016 和 2019
   > - Amazon Linux
   > - Amazon Linux 2
   > - Ubuntu Server 16.04
   > - Ubuntu Server 18.04
   >
   > 在不是从预装代理的 AMI 上创建的 EC2 实例上，必须手动安装代理。有关更多信息，请参阅《Amazon Systems Manager 用户指南》中的以下主题：
   >
   > - 在适用于 Windows Server 的 EC2 实例上安装和配置 SSM 代理
   > - 在适用于 Linux 的 EC2 实例上安装和配置 SSM 代理

3. 按照《Amazon Systems Manager 用户指南》中的配置清单收集中所述启动清单收集。Linux 和 Windows 实例的步骤相同。

   Amazon Config 可以记录以下清单类型的配置变更：

   - 应用程序 – 托管实例的应用程序列表，例如杀毒软件。

- Amazon 组件 – 托管实例的 Amazon 组件列表，例如 Amazon CLI 和开发工具包。
- 实例信息 – 实例信息，例如操作系统名称和版本、域及防火墙状态。
- 网络配置 – 配置信息，例如 IP 地址、网关和子网掩码。
- Windows 更新 – 托管实例的 Windows 更新列表（仅适用于 Windows 实例）。

> **Note**
>
> Amazon Config 目前不支持记录自定义清单类型。

清单收集是众多 Systems Manager 功能之一，这些功能分为运营管理、操作和更改、实例和节点以及共享资源等类别。有关更多信息，请参阅《Amazon Systems Manager 用户指南》中的什么是 Systems Manager？和 Systems Manager 功能。

查找 Amazon Config 发现的资源

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

Looking Up Resources (Console)

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

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在资源清单页面上，为您要查找的资源指定搜索选项：
   - 资源类别 – 选择所有资源类别或将结果范围缩小到仅 Amazon 资源。
   - 资源类型 – 选择所有资源类型或选择要筛选的资源。
   - 合规性 – 选择按任何合规性状态、合规或不合规进行筛选。
3. Amazon Config 列出与您的搜索选项匹配的资源。您可以查看有关资源的以下信息：
   - 资源标识符 – 资源标识符可以是资源 ID，也可以是资源名称（如果适用）。选择资源标识符链接以查看资源详细信息页面。
   - 资源类型 – 列出资源的类型。

- 合规性 – Amazon Config 按照您的规则评估的资源状态。

Looking Up Resources (Amazon CLI)

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

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

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

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

Looking up Resources (API)

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

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。

使用查看Amazon资源的合规信息和评估结果Amazon Config

> **Important**
>
> 要准确报告合规性状态，必须记录 AWS::Config::ResourceCompliance 资源类型。有关更多信息，请参阅录制Amazon资源。

您可以使用Amazon Config控制台或Amazon SDKs 查看资源的合规性信息和评估结果。

主题

- 查看合规性（控制台）
- 查看合规性 (Amazon SDKs)

查看合规性（控制台）

查看合规性（控制台）

1. 登录Amazon Web Services 管理控制台并在家中打开https://console.aws.amazon.com/config/主Amazon Config机。
2. 在Amazon Web Services 管理控制台菜单中，确认区域选择器设置为支持Amazon Config规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 区域和终端节点。
3. 在导航窗格中，选择资源。在“资源”清单页面上，您可以按资源类别、资源类型和合规性状态进行筛选。根据需要选择包括已删除的资源。该表显示了资源类型的资源标识符和该资源的资源合规性状态。资源标识符可以是资源 ID，也可以是资源名称。
4. 从资源标识符列中选择资源。
5. 选择资源时间表按钮。您可以按配置事件、合规性事件或 CloudTrail 事件进行筛选。

> **Note**
>
> 或者，在“资源”清单页面上，您可以直接选择资源名称。要从资源详细信息页面访问资源时间表，请选择资源时间表按钮。

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

查看合规性 (Amazon SDKs)

获取Amazon资源的合规性信息

以下代码示例演示如何使用 `DescribeComplianceByResource`。

CLI

Amazon CLI

获取Amazon资源的合规性信息

以下命令返回Amazon Config 记录的每个违反一条或多条规则的 EC2 实例的合规性信息：

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

在输出中，每个 CappedCount 属性的值都表示该资源违反了多少规则。例如，以下输出表明实例 i-1a2b3c4d 违反了 2 条规则。

输出：

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI命令参考DescribeComplianceByResource中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例检查“COMPLIANT”合规类型的 **AWS::SSM::ManagedInstanceInventory** 资源类型。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

输出：

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeComplianceByResource中的。

适用于 PowerShell V5 的工具

示例 1：此示例检查“COMPLIANT”合规类型的 **AWS::SSM::ManagedInstanceInventory** 资源类型。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

输出：

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeComplianceByResource中的。

获取Amazon资源的合规性摘要

以下代码示例演示如何使用 GetComplianceSummaryByResourceType。

CLI

Amazon CLI

获取所有资源类型的合规性摘要

以下命令返回不合规的Amazon资源数量和合规资源的数量：

```
aws configservice get-compliance-summary-by-resource-type
```

在输出中，每个 CappedCount 属性的值都表示有多少资源合规或不合规。

输出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

获取特定资源类型的合规性摘要

以下命令返回不合规的 EC2 实例数量和合规的实例数量：

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

在输出中，每个 CappedCount 属性的值都表示有多少资源合规或不合规。

输出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI命令参考[GetComplianceSummaryByResourceType](#)中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例返回合规或不合规资源的数量，并将输出转换为 json。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
```

```
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetComplianceSummaryByResourceType中的。

适用于 PowerShell V5 的工具

示例 1：此示例返回合规或不合规资源的数量，并将输出转换为 json。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetComplianceSummaryByResourceType中的。

获取Amazon资源的评估结果

以下代码示例演示如何使用 `GetComplianceDetailsByResource`。

CLI

Amazon CLI

获取Amazon资源的评估结果

以下命令返回 EC2 实例`i-1a2b3c4d`不符合的每条规则的评估结果：

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

输出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI命令参考GetComplianceDetailsByResource中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例提供给定资源的评估结果。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

输出：

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
ResultToken               :
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetComplianceDetailsByResource中的。

适用于 PowerShell V5 的工具

示例 1：此示例提供给定资源的评估结果。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

输出：

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
ResultToken               :
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetComplianceDetailsByResource中的。

使用 Amazon Config 查看 Amazon 资源的合规性历史记录

> **Important**
>
> AWS::Config::ResourceCompliance 资源类型用于存储资源的历史合规性结果。Config 规则无需记录此资源类型即可评估资源或在控制台中查看当前合规状态。
> 记录 AWS::Config::ResourceCompliance 仅允许您在资源时间线中查看历史合规性变化趋势。如果您不需要历史合规性数据，可以排除此资源类型。有关选择要记录的资源的更多信息，请参阅记录 Amazon 资源。

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

主题

- 查看合规性历史记录（控制台）
- 查看合规性历史记录（Amazon CLI）
- 查看资源和规则的合规性历史记录时间线

查看合规性历史记录（控制台）

使用控制台查看合规性历史记录

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

要从资源详细信息页面访问资源时间表，请选择资源时间表按钮。资源时间线将特定资源在一段时间内的更改捕获为。ConfigurationItems您可以按配置事件、合规性事件或 CloudTrail 事件进行筛选。

查看合规性历史记录（Amazon CLI）

使用 Amazon CLI 查看合规性历史记录

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

查看配置历史记录

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

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
```

```
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

有关响应字段的详细解释，请参阅 Components of a Configuration Item 和 支持的资源类型 Amazon Config

来自 Amazon Config 的 Amazon EBS 配置历史记录示例

Amazon Config 会生成一组文件（其中每个文件均代表一个资源类型）并列出 Amazon Config 正在记录的相应类型的资源的所有配置更改。Amazon Config 会将此以资源为中心的配置历史记录导出为您在启用 Amazon 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，其中描述了您的 Amazon Web Services 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"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
```

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

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

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

查看资源和规则的合规性历史记录时间线

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

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

Viewing Resource Timeline Using Resources

通过从资源清单页面中选择特定资源来访问资源时间线。

1. 从左侧导航中选择资源。
2. 在“资源”清单页面上，您可以按资源类别、资源类型和合规性状态进行筛选。根据需要选择包括已删除的资源。

该表显示了资源类型的资源标识符和该资源的资源合规性状态。资源标识符可以是资源 ID，也可以是资源名称。

3. 从资源标识符列中选择资源。
4. 选择资源时间表按钮。您可以按配置事件、合规性事件或 CloudTrail 事件进行筛选。

> **Note**
>
> 或者，在“资源”清单页面上，您可以直接选择资源名称。要从资源详细信息页面访问资源时间表，请选择资源时间表按钮。

Viewing Resource Timeline Using Rules

通过从规则页面中选择特定规则来访问资源时间线。

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

查询 Amazon 资源的合规性历史记录

使用 get-resource-config-history 通过资源类型 `AWS::Config::ResourceCompliance` 查询资源合规性历史记录。

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

您应该可以看到类似于如下所示的输出内容：

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
```

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

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

标记您的 Amazon Config 资源

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

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

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

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

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

与标记相关的限制

下面是适用于标签的基本限制。

限制	描述
每个资源的最大标签数	50
最大密钥长度	128 个 Unicode 字符（采用 UTF-8 格式）
最大值长度	256 个 Unicode 字符（采用 UTF-8 格式）
前缀限制	请勿在标签名称或值中使用 `aws:` 前缀，因为它专为 Amazon 使用预留。您无法编辑或删除带此前缀的标签名称或值。具有此前缀的标签不计入每个资源的标签数限制。
字符限制	标签只能包含 Unicode 字母、数字、空格或以下符号：`_ . : / = + - @`

使用 Amazon Config API 操作管理标签

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

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource` 和 `UntagResource` 需要某些 Amazon Identity and Access Management（IAM）权限才能控制访问权限。有关更多信息，请参阅《IAM 用户指南》中的根据标签键控制访问权限。

使用 Amazon Config 规则评估资源

Amazon Config 用于评估 Amazon 资源的配置设置。为此，您可以创建 Amazon Config 规则，这些规则代表您的理想配置设置。 Amazon Config 提供名为托管规则的可自定义预定义规则，以帮助您入门。

主题

- 注意事项
- 区域支持
- Amazon Config 规则的组成部分
- Amazon Config 托管规则
- Amazon Config 自定义规则
- 服务相关的 Amazon Config 规则
- 添加 Amazon Config 规则
- 更新 Amazon Config 规则
- 删除 Amazon Config 规则
- 查看 Amazon Config 规则的详细信息和合规性信息
- 为 Amazon Config 规则开启主动评估
- 向 Security Hub CSPM 发送规则评估
- 使用 Amazon Config 规则评估资源
- 从 Amazon Config 规则中删除评估结果
- Amazon Config 规则疑难解答

注意事项

Cost Considerations

有关资源记录相关费用的详细信息，请参阅 Amazon Config 定价。

建议：在删除规则之前，请考虑将 **`AWS::Config::ResourceCompliance`** 资源类型排除在记录范围之外

删除规则会创建配置项目 (CIs)`AWS::Config::ResourceCompliance`，这可能会影响配置记录器的成本。如果您要删除评估大量资源类型的规则，则可能会导致 CIs 记录的资源数量激增。

为避免相关费用，您可以选择在删除规则之前禁用 AWS::Config::ResourceCompliance 资源类型的记录，并在删除规则后重新启用记录。

不过删除规则是一个异步过程，因此可能需要一个小时或更长时间才能完成。在对 AWS::Config::ResourceCompliance 禁用记录期间，将不会在关联资源的历史记录中记录规则评估。

Amazon Config 建议您在决定如何继续删除规则之前， case-by-case先权衡这些因素。

建议：添加逻辑来处理对自定义 Lambda 规则的资源的评估

在创建 Amazon Config 自定义 lambda 规则时，强烈建议您添加逻辑来处理已删除资源的评估。

当评估结果被标记为 NOT_APPLICABLE 时，这些资源将被标记为已删除并被清理。如果未将其标记为NOT_APPLICABLE，则在删除规则之前，评估结果将保持不变，这可能会导致删除规则AWS::Config::ResourceCompliance后创建 CIs 的for出现意外激增。

有关如何设置 Amazon Config 自定义 lambda 规则以返回NOT_APPLICABLE已删除资源的信息，请参阅使用 Amazon Config 自定义 lambda 规则管理已删除的资源。

建议：为自定义 Lambda 规则提供范围内的资源

Amazon Config 如果自定义 Lambda 规则的范围不限于一种或多种资源类型，则该规则可能会导致大量的 Lambda 函数调用。为避免与您的账户相关的活动增加，强烈建议提供自定义 Lambda 规则范围内的资源。如果未选择任何资源类型，该规则将为账户中的所有资源调用 Lambda 函数。

Other considerations

托管规则的默认值

只有在使用 Amazon 控制台时，才会预先填充为托管规则指定的默认值。未提供 API、CLI 或 SDK 的默认值。

配置项目记录延迟

Amazon Config 通常会在检测到更改后立即或按您指定的频率记录对资源的配置更改。但是，这需要尽最大努力，有时可能需要更长的时间。例如，具有已知延迟的资源类型是 AWS::SecretsManager::Secret 此资源类型只是一个示例，此列表并非详尽无遗。

策略与合规结果

在中管理@@ 的 IAM 策略和其他策略 Amazon Organizations可能会影响您是否 Amazon Config 有权记录资源的配置更改。此外，规则会直接评估资源的配置，且执行评估时不会考虑这些策略。确保现行策略与您打算使用 Amazon Config的方式保持一致。

资源类型的标签支持

如果资源类型不支持标记或在其 describe API 响应中不包含标签信息，则 Amazon Config 不会在该资源类型的配置项目 (CIs) 中捕获标签数据。 Amazon Config 仍将记录这些资源。但是，任何依赖标签数据的功能都将无法使用。这会影响依赖标签数据的基于标签的筛选、分组或合规性评估。

不支持目录存储桶

在评估 Amazon Simple Storage Service（Amazon S3）资源时，托管规则仅支持通用存储桶。有关通用存储桶和目录存储桶的更多信息，请参阅 Amazon S3 用户指南中的存储桶概述和目录存储桶。

托管规则和全局 IAM 资源类型

2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 Amazon Amazon Config 区域 Amazon Config 中进行记录。2022 年 2 月 Amazon Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 Amazon 资源 | 全球资源。

如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。

为避免不必要的评估，您应仅将报告全局 IAM 资源类型合规性的定期规则部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

区域支持

目前，以下 Amazon 区域支持 Amazon Config 规则功能。有关哪些区域支持哪些单独 Amazon Config 规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

区域名称	区域	端点	协议	
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
		config-fips.us-east-2.amazonaws.com	HTTPS	

区域名称	区域	端点	协议
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
美国西部（北加利福尼亚）	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
亚太地区（马来西亚）	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（新西兰）	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（台北）	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
亚太地区（泰国）	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
亚太地区（东京）	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
中国（北京）	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS

区域名称	区域	端点	协议	
中国（宁夏）	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS	
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
墨西哥（中部）	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议	
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS	
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

以下区域支持跨 Amazon 组织成员账户部署 Amazon Config 规则。

区域名称	区域	端点	协议	
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
美国西部（北加利福尼亚）	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议	
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
亚太地区（马来西亚）	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS	
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
亚太地区（新西兰）	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS	
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS	

区域名称	区域	端点	协议	
亚太地区（台北）	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS	
亚太地区（泰国）	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS	
亚太地区（东京）	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS	
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS	
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS	
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	

区域名称	区域	端点	协议
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS
墨西哥（中部）	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

Amazon Config 规则的组成部分

Amazon Config 规则会评估您的 Amazon 资源的配置设置。本页讨论规则的组成部分。

主题

- Amazon Config 规则是如何运作的
- 触发器类型
- 评估模式
- Amazon Config 规则元数据

Amazon Config 规则是如何运作的

在 Amazon Config 持续跟踪您的资源中出现的配置更改时，它会检查这些更改是否不符合规则中的任何条件。如果资源不符合规则，则会将该资源和规则 Amazon Config 标记为不合规。

Amazon Config 一条规则有四种可能的评估结果。

评估结果	描述
COMPLIANT	规则通过了合规性检查的条件。
NON_COMPLIANT	此规则未通过合规性检查的条件。
ERROR	其中一个 required/optional 参数无效、类型不正确或格式不正确。
NOT_APPLICABLE	用于筛选出无法应用规则逻辑的资源。例如，该alb-desync-mode-check规则仅检查应用程序负载均衡器，而忽略网络负载均衡器和网关负载均衡器。

例如，在创建 EC2 卷时， Amazon Config 可以根据要求对卷进行加密的规则来评估该卷。如果卷未加密，则会将该卷和规则 Amazon Config 标记为不合规。 Amazon Config 还可以检查您的所有资源以了解整个账户的需求。例如， Amazon Config 可以检查账户中的 EC2 卷数是否保持在所需的总数之内，或者某个账户是否 Amazon CloudTrail 用于日志记录。

触发器类型

向账户添加规则后， Amazon Config 将您的资源与规则的条件进行比较。在这次初始评估之后，每次触发评估时都会 Amazon Config 继续运行评估。规则中会定义评估触发器，可以包括以下类型。

触发器类型	描述
配置更改	Amazon Config 当存在与规则范围匹配的资源并且资源的配置发生变化时，会对规则进行评估。评估将在 Amazon Config 发送配置项目变更通知后运行。

触发器类型	描述
	通过定义规则的范围来选择哪些资源启动评估。范围可以包括： • 一个或多个资源类型 • 资源类型和资源 ID 的组合 • 标签键和值的组合 • 当创建、更新或删除任何记录的资源时 Amazon Config 当它检测到与规则范围相匹配的资源发生变化时，就会运行评估。您可以使用范围来定义哪些资源启动评估。
定期	Amazon Config 按您选择的频率对规则进行评估；例如，每 24 小时运行一次。
混合	有些规则既有配置更改也有定期触发器。对于这些规则，它 Amazon Config 会在检测到配置更改时以及按照您指定的频率评估您的资源。

评估模式

Amazon Config 规则有两种评估模式。

评估模式	描述
主动	使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 Amazon 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。
侦查	使用侦查评估来评估已部署的资源。这允许您评估现有资源的配置设置。

> **Note**
>
> 主动规则不会修复标记为 NON_COMPLIANT 的资源，也不会阻止部署这些资源。

有关更多信息，请参阅为 Amazon Config 规则开启主动评估。

主动评估的托管规则列表

有关支持主动评估的托管规则列表，请参阅按评估模式列出的 Amazon Config 托管规则列表。

支持主动评估的资源类型列表

以下是支持主动评估的资源类型列表：

- `AWS::EC2::EIP`

Amazon Config 规则元数据

Amazon Config 规则可以包含以下可变元数据：

默认名称

defaultName 是规则实例在默认情况下将获得的名称。

描述

规则描述提供了规则评估内容的上下文。 Amazon Config 控制台具有 256 个字符的限制。作为最佳实践，规则描述应以“检查是否”开头，并包括对 NON_COMPLIANT 场景的描述。在规则描述中首次提及时，服务名称应以 Amazon 或 Amazon 开头。例如， Amazon CloudTrail 或者用 Amazon CloudWatch 代替 CloudTrail 或 CloudWatch 首次使用。服务名称可以在后续引用后使用缩写。

范围

范围决定了规则所针对的资源类型。有关支持的资源类型列表，请参阅支持的资源类型。

compulsoryInputParameter详细信息

compulsoryInputParameter详细信息用于规则进行评估所需的参数。例如，`access-keys-rotated` 托管规则包含 `maxAccessKeyAge` 作为必要参数。如果为必要参数，则不会被标记为（可选）。必须指定每个参数的类型。类型可以是 “字符串”、“整数”、“双精度”、“CSV”、“布尔值” 和 “StringMap” 之一。

optionalInputParameter详细信息

optionalInputParameter详细信息用于规则评估时可选的参数。例如，`elasticsearch-logs-to-cloudwatch` 托管规则包含 `logTypes` 作为可选参数。必须指定每个参数的类型。类型可以是“字符串”、“整数”、“双精度”、“CSV”、“布尔值” 和 “StringMap” 之一。

supportedEvaluationModes

supportedEvaluationModes 决定何时对资源进行评估，无论是在部署资源之前，还是在部署资源之后。

`DETECTIVE` 用于评估已经部署的资源。这允许您评估现有资源的配置设置。`PROACTIVE` 用于在资源部署之前对其进行评估。

这使您可以评估一组资源属性（如果用于定义 Amazon 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。

您可以指定 to supportedEvaluationModes `DETECTIVE` `PROACTIVE`、或两者兼`DETECTIVE`而有之`PROACTIVE`。必须指定评估模式，且此字段不能为空。

> **Note**
>
> 主动规则不会修复标记为 NON_COMPLIANT 的资源，也不会阻止部署这些资源。

Amazon Config 托管规则

Amazon Config 提供了 Amazon 托管规则（可自定义的预定义规则），Amazon Config 使用这些规则来评估您的 Amazon 资源是否符合常见的最佳实践。例如，您可以使用一个托管规则来快速开始评估您的 Amazon Elastic Block Store（Amazon EBS）卷是否已加密，或者特定标签是否已应用于您的资源。

Amazon Config 控制台可以引导您完成托管规则的配置和激活过程。您还可以使用 Amazon Command Line Interface 或 Amazon Config API 来传递用于定义托管规则配置的 JSON 代码。

您可以自定义托管规则的行为以满足您的需求。例如，您可以定义规则的范围以便限定触发规则评估的资源，例如 EC2 实例或卷。

您可以自定义规则的参数，以便定义您的资源为符合规则而必须具备的属性。例如，您可以自定义一个参数，以指定您的安全组应阻止传输到特定端口号的传入流量。

在使用托管规则之前，请参阅 注意事项

主题

- Amazon Config 托管规则列表
- 按评估模式列出的 Amazon Config 托管规则列表
- 按触发器类型列出的 Amazon Config 托管规则列表
- 按区域可用性列出的 Amazon Config 托管规则列表
- 使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则

Amazon Config 托管规则列表

Amazon Config 目前支持以下托管规则。在使用这些规则之前，请参阅 注意事项

主题

- access-keys-rotated
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-重定向检查
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-execution-logging-已启用
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-休息
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-记录
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-environment-privileged-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-report-group-encrypted-在休息时
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-task-logging-enabled
- dax-encryption-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-记录
- dms-replication-task-targetdb-记录
- docdb-cluster-encrypted-in-交通
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-deletion-protection-已启用
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-管理instance-managed-by-systems器
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance

- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-auto-minor-version-升级检查
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中

- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl 检查
- emr-kerberos-enabled
- emr-master-no-public-ip
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-ontap-deployment-type-检查
- fsx-openzfs-deployment-type-检查
- fsx-windows-deployment-type-检查
- glue-job-logging-enabled
- glue-spark-job-supported-版本
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms 动作
- iam-inline-policy-blocked-kms 动作
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-检查

- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- restricted-ssh
- ec2-instances-in-vpc
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- mfa-enabled-for-iam-控制台访问权限
- mq-active-deployment-mode
- mq-auto-minor-version-已启用升级
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-需要-tls
- msk-unrestricted-access-check
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-subnet-change-protection-已启用
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-enhanced-monitoring-enabled
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-instance-encrypted在途中
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-sqlserver-encrypted-in-交通

- rds-sql-server-logs到云端观察
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-routes-在 vpc 内
- required-tags
- restricted-common-ports
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-启用日志功能
- subnet-auto-assign-public-ip 已禁用
- transfer-connector-logging-enabled
- vpc-endpoint-enabled
- vpc-flow-logs-enabled

- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

access-keys-rotated

检查活动 IAM 访问密钥是否在 maxAccessKeyAge 中指定的天数内轮换（更改）。如果访问密钥未在指定时间段内轮换，则此规则为 NON_COMPLIANT。默认值为 90 天。

Warning

请不要向未经授权方提供访问密钥，即便是为了帮助找到您的账户标识符也不行。通过这样做，您可以授予他人永久访问您的帐户的权限。安全最佳实践是，在用户不再需要密码和访问密钥时将其删除。

Note

控制台中标记为“不合规”的资源类型
如果此规则发现您的任何访问密钥不合规，则该AWS::IAM::User资源类型也将在控制台中标记为不合规。 Amazon
托管规则和全局 IAM 资源类型
2022 年 2 月之前加入的全球 IAM 资源类型
（AWS::IAM::GroupAWS::IAM::Policy、AWS::IAM::Role、和AWS::IAM::User）
只能在 2022 年 2 月之前可用的 Amazon Amazon Config 区域 Amazon Config 中进行记录。2022 年 2 月 Amazon Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 Amazon 资源 | 全球资源。
如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。
为避免不必要的评估，您应仅将报告全局 IAM 资源类型合规性的定期规则部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

限制
此规则不适用于 Amazon 账户根用户访问密钥。要删除或轮换您的根用户访问密钥，请使用您的根用户凭据登录到位于的 “我的安全证书” 页面https://www.amazonaws.cn/console/。Amazon Web Services 管理控制台

标识符：ACCESS_KEYS_ROTATED

资源类型： AWS::IAM::User

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

maxAccessKey年龄, 类型：int, 默认值：90

最长不轮换天数。默认值：90。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

acm-certificate-expiration-check

检查您账户中的 Certifice Manager Amazon 证书是否被标记为在指定的天数内到期。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。如果您的证书即将过期，则此规则为 NON_COMPLIANT。

标识符：ACM_CERTIFICATE_EXPIRATION_CHECK

资源类型： AWS::ACM::Certificate

触发器类型：配置更改和定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

daysToExpiration （可选）, 类型：int, 默认值：14

指定规则将 ACM 证书标记为不合规之前的天数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

active-mq-supported-version

检查 Amazon MQ ActiveMQ 代理是否在指定的最低支持引擎版本上运行。如果 ActiveMQ 代理未在您指定的最低支持引擎版本上运行，此规则为 NON_COMPLIANT。

标识符：ACTIVE_MQ_SUPPORTED_VERSION

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（海得拉巴）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

supportedEngineVersion, 类型：字符串

用于检查 ActiveMQ 代理支持的最低引擎版本的规则的字符串值。ActiveMQ 代理使用语义版本控制规范：X.Y.Z。X 代表主要版本，Y 代表次要版本，Z 代表补丁版本。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

alb-desync-mode-check

检查应用程序负载均衡器（ALB）是否已配置为用户定义的取消同步缓解模式。如果 ALB 取消同步缓解模式与用户定义的取消同步缓解模式不匹配，则此规则为 NON_COMPLIANT。

标识符：ALB_DESYNC_MODE_CHECK

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

desyncMode, 类型：CSV

逗号分隔列表，客户可选择其中的最多 2 个值：“defensive”、“strictest”和“monitor”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

alb-http-to-https-重定向检查

检查是否在应用程序负载均衡器的所有 HTTP 侦听器上都配置了 HTTP 到 HTTPS 重定向。如果应用程序负载均衡器的一个或多个 HTTP 侦听器未配置 HTTP 到 HTTPS 重定向，则此规则为 NON_COMPLIANT。如果多个 HTTP 侦听器中的一个转发到 HTTP 侦听器而不是重定向，则此规则也为 NON_COMPLIANT。

标识符：ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

api-gwv2-access-logs-enabled

检查 Amazon API Gateway V2 阶段是否启用了访问日志功能。如果阶段配置中不存在“accessLogSettings”，则该规则不兼容。

标识： API_GWV2_ACCESS_LOGS_ENABLED

资源类型： AWS::ApiGatewayV2::Stage

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

api-gwv2-authorization-type-configured

检查 Amazon API Gatewayv2 API 路由是否设置了授权类型。如果授权类型为 NONE，则此规则为 NON_COMPLIANT。

标识符： API_GWV2_授权类型_ 已配置

资源类型： AWS::ApiGatewayV2::Route

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

authorizationType（可选）, 类型：字符串

用于检查 API 路由的授权类型的参数。与 CUSTOM、 Amazon_IAM、JWT 匹配的字符串参数有效。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

api-gw-execution-logging-已启用

检查 Amazon API Gateway 阶段中的所有方法是否均已启用日志记录。如果未启用日志记录，或者 `loggingLevel` 既不是 ERROR 也不是 INFO，则此规则为 NON_COMPLIANT。

标识符： API_GW_执行_日志 _启用

资源类型： AWS::ApiGateway::Stage， AWS::ApiGatewayV2::Stage

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

loggingLevel（可选）, 类型：字符串, 默认值：ERROR、INFO

特定日志记录级别的逗号分隔列表（例如，ERROR, INFO 或 ERROR,INFO）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

api-gw-ssl-enabled

检查 REST API 阶段是否使用 SSL 证书。如果 REST API 阶段没有关联的 SSL 证书，则此规则为 NON_COMPLIANT。

> **Note**
>
> NOT_APPLICABLE如果 GetIntegrationAPI 返回的集成类型不是 a HTTP s 类型，则返回此规则。此规则评估 API Gateway 阶段设置中的 SSL 证书配置，而不是实际部署状态。

标识符： API_GW_SSL_EN ABLED

资源类型： AWS::ApiGateway::Stage

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

证书IDs （可选），类型：CSV

在 REST API 阶段 IDs 配置的以逗号分隔的客户端证书列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

approved-amis-by-id

检查 EC2 实例是否使用指定的 Amazon 系统映像 (AMIs)。指定已批准的 AMI 列表 IDs。不在此列表中的正在运行的实例不合规。 AMIs

标识符：APPROVED_AMIS_BY_ID

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

amiIds, 类型：CSV

以逗号分隔的列表，最多包含 21 个 AMI。 IDs不能超过 1024 个字符。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

approved-amis-by-tag

检查 EC2 实例是否使用指定的 Amazon 系统映像 (AMIs)。指定标识的标签 AMIs。如果运行的实例没有至少一个指定标签 AMIs ，则属于 NON_COMPLIMENT。

标识符：APPROVED_AMIS_BY_TAG

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

amisByTagKeyAndValue, 类型： StringMap, 默认：标签键：标签值，other-tag-key

以逗号分隔的列表，最多包含 10 个 AMIs 标签（标签键:tag-value）。例如，tag-key1 AMIs 与 tag-key1 匹配；tag-key2：value2 匹配值为 2 的 tag-key2。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

appsync-associated-with-waf

检查 Amazon AppSync APIs 是否与 Amazon WAFv2 Web 访问控制列表相关联 (ACLs)。如果 Amazon AppSync API 未与 Web ACL 关联，则该规则不合规。

标识符：APPSYNC_ASSOCIATED_WITH_WAF

资源类型： AWS::AppSync::GraphQLApi

触发器类型： 定期

Amazon Web Services 区域：除亚太地区（泰国）、亚太 Amazon 地区（雅加达）、非洲（开普敦）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）、（美国东部）、（美国西部）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里） Amazon GovCloud 、欧洲（西班牙苏黎世） Amazon GovCloud 、欧洲（西班牙）、欧洲（苏黎世）、欧洲（西班牙）、欧洲（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（西班牙）) 区域

参数：

wafWebAclARNs （可选）, 类型：CSV

以逗号分隔的授权网站的 Amazon 资源名称 (ARNs) 列表。 ACLs

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

appsync-authorization-check

检查 Amazon AppSync API 是否使用允许的授权机制。如果使用的是未经批准的授权机制，则此规则为 NON_COMPLIANT。

标识符：APPSYNC_AUTHORIZATION_CHECK

资源类型： AWS::AppSync::GraphQLApi

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

AllowedAuthorizationTypes, 类型：CSV

以逗号分隔的允许 Amazon AppSync 授权机制列表。允许的值为：''、'_LAMBDA'、API_KEY '_Amazon IAM'、'Amazon OPENID_CONNECT'、'AMAZON_COGNITO_USER_POOLS '。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

appsync-logging-enabled

检查 Amazon AppSync API 是否启用了字段级日志记录。如果未启用字段级日志记录，或者 AppSync API 的字段日志记录级别与 “`fieldLoggingLevel`” 参数中指定的值不匹配，则该规则不合规。

标识符：APPSYNC_LOGGING_ENABLED

资源类型： AWS::AppSync::GraphQLApi

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

fieldLoggingLevel （可选）, 类型：CSV

规则要检查的字段日志记录级别的逗号分隔列表。例如，“ERROR, INFO”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

athena-workgroup-encrypted-at-休息

检查 Amazon Athena 工作组是否启用了静态加密。如果未为 Athena 工作组启用静态数据加密，则此规则为 NON_COMPLIANT。

标识符：ATHENA_WORKGROUP_ENCRYPTED_AT_REST

资源类型： AWS::Athena::WorkGroup

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部） Amazon GovCloud 、（美国西部） Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

athena-workgroup-logging-enabled

检查亚马逊 Ath WorkGroup ena 是否向亚马逊发布使用量指标。 CloudWatch如果将 WorkGroup Amazon Athena PublishCloudWatchMetricsEnabled “” 设置为 false，则该规则不合规。

标识符：ATHENA_WORKGROUP_LOGGING_ENABLED

资源类型： AWS::Athena::WorkGroup

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

aurora-mysql-cluster-audit-记录

检查 Amazon Aurora MySQL 数据库集群是否启用了审核日志记录。如果数据库集群未启用审核日志记录，则此规则为 NON_COMPLIANT。

标识符：AURORA_MYSQL_CLUSTER_AUDIT_LOGGING

资源类型： AWS::RDS::DBCluster

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

autoscaling-launchconfig-requires-imdsv2

检查是否只启 IMDSv2 用。如果启动配置中未包含元数据版本，或者同时启用了元数据 V1 和 V2，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_LAUN CHCONFIG_requ IMDSV2

资源类型： AWS::AutoScaling::LaunchConfiguration

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

autoscaling-launch-config-hop-极限

检查元数据令牌可以传输的网络跃点数。如果元数据响应跃点限制大于 1，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

资源类型： AWS::AutoScaling::LaunchConfiguration

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、亚太地区（雅加达）、亚太地区（马来西亚） Amazon GovCloud 、（美国东部）、（美国西部） Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

autoscaling-launch-template

检查是否根据 EC2 启动模板创建了亚马逊弹性计算云 (EC2) Auto Scaling 组。如果伸缩组不是根据 EC2 启动模板创建的，则该规则为 NON_Complift。

标识符：AUTOSCALING_LAUNCH_TEMPLATE

资源类型： AWS::AutoScaling::AutoScalingGroup

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

autoscaling-multiple-az

检查 Auto Scaling 组是否跨越多个可用区。如果 Auto Scaling 组不跨越多个可用区，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_MULTIPLE_AZ

资源类型： AWS::AutoScaling::AutoScalingGroup

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

minAvailabilityZones （可选）, 类型：int

预期可用区的最小数量。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

autoscaling-multiple-instance-types

检查 Amazon A EC2 uto Scaling 组是否使用多种实例类型。如果 Amazon A EC2 uto Scaling 组仅定义了一个实例类型，则该规则不合规。此规则不评估基于属性的实例类型。

标识符：AUTOSCALING_MULTIPLE_INSTANCE_TYPES

资源类型： AWS::AutoScaling::AutoScalingGroup

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

clb-desync-mode-check

检查经典负载均衡器（CLB）是否配置了用户定义的取消同步缓解模式。如果 CLB 取消同步缓解模式与用户定义的取消同步缓解模式不匹配，则此规则为 NON_COMPLIANT。

标识符：CLB_DESYNC_MODE_CHECK

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

desyncMode, 类型：CSV

值的逗号分隔列表。您最多可以选择两个。有效值包括“Defensive”、“Strictest”和“Monitor”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

clb-multiple-az

检查 Classic Load Balancer 是否跨越多个可用区 (AZs)。如果 Classic Load Balancer 的跨度小于 2 AZs 或未跨越`minAvailabilityZones`参数中 AZs 提及的数量（如果提供），则该规则不合规。

标识符：CLB_MULTIPLE_AZ

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

minAvailabilityZones （可选）, 类型：int

期望的最小数量 AZs。有效值介于 2 到 10 之间，包括 2 和 10。如果未指定参数，则默认值为 2。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudformation-stack-drift-detection-检查

检查 Amazon CloudFormation (Amazon CloudFormation) 堆栈的实际配置是否与预期配置不同或有所偏差。如果堆栈的一个或多个资源与其预期配置不同，则将堆栈视为已偏离。当堆栈偏差

状态为 IN_SYNC 时，规则和堆栈都是 COMPLIANT。当堆栈偏离状态为 DRIFTED 时，规则为 NON_COMPLIANT。

> **Note**
>
> 此规则对您账户中的每个堆栈执行 DetectStackDrift 操作。该 DetectStackDrift 操作最多可能需要几分钟，具体取决于堆栈中包含的资源数量。鉴于此规则的最长执行时间限制为 15 分钟，因此此规则可能会在完成对您账户中所有堆栈的评估之前超时。
> 如果您遇到此问题，建议您使用标签来限制规则范围内的堆栈数量。您可执行以下操作：
>
> 1. 将您的堆栈分成几组，每个组有一个不同的标签。
> 2. 将相同的标签应用于该组中的所有堆栈。
> 3. 在您的账户中设置此规则的多个实例，每个实例使用不同的标签。这允许规则的每个实例仅处理具有其作用域中提及的相应标签的堆栈。

标识符：CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

资源类型： AWS::CloudFormation::Stack

触发器类型：配置更改和定期

Amazon Web Services 区域：除亚太 Amazon 地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（海得拉巴）、亚太地区（墨尔本）、以色列（特拉维夫）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

cloudformationRoleArn, 类型：字符串

具有策略权限的 IAM 角色的 Amazon 资源名称 (ARN)，用于检测堆栈偏差。 Amazon CloudFormation 有关该角色所需 IAM 权限的信息，请参阅《Amazon CloudFormation 用户指南》中的检测堆栈和资源的非受管配置更改 | 检测偏差时的注意事项。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudformation-stack-service-role-检查

检查 Amazon CloudFormation 堆栈是否在使用服务角色。如果 CloudFormation 堆栈没有与之关联的服务角色，则该规则为 NON_COMPLIME。

标识符：CLOUDFORMATION_STACK_SERVICE_ROLE_

资源类型： AWS::CloudFormation::Stack

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudformation-termination-protection-check

检查 Amazon CloudFormation 堆栈是否启用了终止保护。如果堆栈上未启用终止保护，则此规则不合规。 CloudFormation

标识符：CLOUDFORMATION_TERMINATION_P

资源类型： AWS::CloudFormation::Stack

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudtrail-s3-bucket-access-logging

检查您的 Amazon CloudTrail 日志的 S3 存储桶配置是否启用了 Amazon S3 服务器访问日志记录。如果 CloudTrail 跟踪的至少一个 S3 存储桶未启用 S3 服务器访问日志记录，则该规则不合规。

标识符：CLOUDTRAIL_S3_BUCKET_ACCESS_LOGGING

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudtrail-s3-bucket-public-access-prohibited

检查您的 Amazon CloudTrail 日志的 S3 存储桶配置是否阻止了公共访问。如果 CloudTrail 跟踪中至少有一个可公开访问的 S3 存储桶，则该规则不合规。

标识符：CLOUDTRAIL_S3_BUCKET_PUBLIC_ACCESS_PROHIBITED

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudtrail-s3-dataevents-enabled

检查是否至少有一个 Amazon CloudTrail 跟踪记录了所有 S3 存储桶的亚马逊简单存储服务 (Amazon S3) Service 数据事件。如果有跟踪或者没有跟踪记录 S3 数据事件，则此规则为 NON_COMPLIANT。

标识符：CLOUDTRAIL_S3_DATAEVENTS_ENABLED

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

S3BucketNames （可选），类型：字符串

> 逗号分隔的 S3 存储桶名称列表，应为其启用数据事件日志记录。默认行为会检查所有 S3 存储桶。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudtrail-security-trail-enabled

检查是否至少有一 Amazon CloudTrail 条使用安全最佳实践定义的跟踪。如果至少有一个跟踪满足以下所有条件，则此规则为 COMPLIANT：

- 记录全局服务事件
- 是一个多区域跟踪
- 已启用日志文件验证
- 使用 KMS 密钥加密
- 记录读取和写入事件
- 记录管理事件
- 不排除任何管理事件

如果没有跟踪符合上述所有条件，则此规则为 NON_COMPLIANT。

标识符：CLOUDTRAIL_SECURITY_TRAIL_ENABLED

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudwatch-alarm-action-check

检查 CloudWatch 警报是否为 “警报”、“数据不足” 或 “正常” 状态配置了操作。（可选）检查是否有任何操作与指定 ARN 匹配。如果没有为警报或可选参数指定任何操作，则此规则为 NON_COMPLIANT。

标识符：CLOUDWATCH_ALARM_ACTION_CHECK

资源类型： AWS::CloudWatch::Alarm

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

okActionRequired, 类型：字符串, 默认：false

当警报从任意其他状态转换为 OK 状态时，警报至少有一个操作。

insufficientDataAction必填项, 类型：字符串, 默认：True

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。

alarmActionRequired, 类型：字符串, 默认：True

警报具有至少一个操作。

action1（可选）, 类型：字符串

要执行的操作，指定为 ARN。

action2（可选）, 类型：字符串

要执行的操作，指定为 ARN。

action3（可选）, 类型：字符串

要执行的操作，指定为 ARN。

action4（可选）, 类型：字符串

要执行的操作，指定为 ARN。

action5（可选）, 类型：字符串

要执行的操作，指定为 ARN。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudwatch-alarm-action-enabled-检查

检查 Amazon CloudWatch 警报操作是否处于启用状态。如果 CloudWatch 警报操作未处于启用状态，则该规则为 “不合规”。

标识符：CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

资源类型： AWS::CloudWatch::Alarm

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部） Amazon GovCloud 、（美国西部） Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudwatch-alarm-resource-check

检查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、Amazon RDS 集群或 S3 存储桶。如果指定指标具有资源 ID 和 CloudWatch 警报，则该规则合规。

标识符：CLOUDWATCH_ALARM_RESOURCE_CHECK

资源类型： AWS::EC2::Instance、 AWS::RDS::DBCluster、 AWS::S3::Bucket、 AWS::EC2::Volume

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

resourceType, 类型：字符串

Amazon 资源类型。该值可以是以下值之一： AWS::EC2::Volume AWS::EC2::Instance、AWS::RDS::DBCluster、或 AWS::S3::Bucket。

metricName, 类型：字符串

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

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudwatch-log-group-encrypted

检查 Amazon CloudWatch 日志组是否使用任何 Amazon KMS 密钥或指定的 K Amazon MS 密钥 ID 进行加密。如果 CloudWatch 日志组未使用 KMS 密钥加密，或者使用规则参数中未提供的 KMS 密钥进行加密，则该规则不合规。

标识符：CLOUDWATCH_LOG_GROUP_ENCRYPTED

资源类型： AWS::Logs::LogGroup

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

KmsKeyId （可选），类型：字符串

用于加密日志组的 KMS 密钥的 ID 的 Amazon 资源名称（ARN）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloud-trail-cloud-watch-启用日志

检查是否将 Amazon CloudTrail 跟踪配置为向日志发送 CloudWatch 日志。如果跟踪的 CloudWatchLogsLogGroupArn 属性为空，则该跟踪不兼容。

标识符：CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

expectedDeliveryWindow年龄（可选），类型：int

最近一次向符合合规性的 CloudWatch 日志交付的最大时长（以小时为单位）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloudtrail-enabled

> **Important**
>
> 对于此规则，规则标识符（CLOUD_TRAIL_ENABLED）和规则名称（cloudtrail-enabled）是不同的。

检查您的 Amazon 账户中是否启用了 Amazon CloudTrail 跟踪。如果跟踪未启用，则规则为 NON_COMPLIANT。或者，该规则会检查特定的 S3 存储桶、亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题和日志组 CloudWatch 。

标识符：CLOUD_TRAIL_ENABLED

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

s3BucketName （可选），类型：字符串

用于 CloudTrail 向其传送日志文件的 S3 存储桶的名称。

snsTopicArn （可选），类型：字符串

CloudTrail 用于通知的 SNS 主题 ARN。

cloudWatchLogsLogGroupArn （可选），类型：字符串

CloudWatch CloudTrail 要向其发送数据的日志组 ARN。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloud-trail-encryption-enabled

检查 Amazon CloudTrail 是否配置为使用服务器端加密 (SSE) Amazon Key Management Service (Amazon KMS) 加密。如果定义了，则该规则 KmsKeyId 是合规的。

标识符：CLOUD_TRAIL_ENCRYPTION_ENABLED

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cloud-trail-log-file-已启用验证

检查是否 Amazon CloudTrail 创建了带有日志的签名摘要文件。 Amazon 建议必须在所有轨迹上启用文件验证。如果未启用验证，则此规则为 NON_COMPLIANT。

标识符：CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cmk-backing-key-rotation-已启用

检查是否为每个密钥启用了自动密钥轮换，并与客户创建的 KMS 密钥的密 Amazon 钥 ID 相匹配。如果资源的 Confi Amazon g 记录器角色没有权限，则该 kms:DescribeKey 规则不合规。

> **Note**
>
> 对于非对称 KMS 密钥、HMAC KMS 密钥、带有导入密钥材料的 KMS 密钥或自定义密钥存储区中的 KMS 密钥，不支持自动密钥轮换。

标识符：CMK_BACKING_KEY_ROTATION_ENABLED

资源类型： AWS::KMS::Key

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

codebuild-project-environment-privileged-检查

检查 Amazon CodeBuild 项目环境是否启用了特权模式。如果 “权限模式” 设置为 “true”，则 CodeBuild 该项目规则不合规。

标识符：CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

exemptedProjects（可选）, 类型：CSV

允许具有 “权限模式” 且值为 “true” 的 CodeBuild 项目名称的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

codebuild-project-logging-enabled

检查 Amazon CodeBuild 项目环境是否至少启用了一个日志选项。如果所有现有日志配置的状态都设置为“DISABLED”，则此规则为 NON_COMPLIANT。

标识符：CODEBUILD_PROJECT_LOGGING_ENABLED

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、亚太地区（雅加达）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

s3BucketNames （可选）, 类型：字符串

逗号分隔的 Amazon S3 存储桶名称列表，如果配置了 S3 日志，则应将日志发送到这些存储桶。

cloudWatchGroup姓名（可选），类型：字符串

以逗号分隔的 Amazon CloudWatch 日志组名称列表，如果配置了日志，则应将 CloudWatch 日志发送到这些名称。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

codebuild-project-s3 个日志加密

检查配置了 Amazon S3 日志的 Amazon CodeBuild 项目是否为其日志启用了加密。如果在项目的 S3 LogsConfig 中将 “encryptionDisabled” 设置为 “true”，则该规则不合规。 CodeBuild

标识符：CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、亚太地区（雅加达）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

exemptedProjects（可选），类型：CSV

允许输出未加密日志的 CodeBuild 项目名称列表，以逗号分隔。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

codebuild-report-group-encrypted-在休息时

检查 Amazon CodeBuild 报告组是否启用了静态加密设置。如果 “” 为 “真EncryptionDisabled”，则该规则不合规。

标识符：CODEBUILD_REPORT_GROUP_ENCRYPTED_AT_REST

资源类型： AWS::CodeBuild::ReportGroup

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

custom-eventbus-policy-attached

检查 Amazon EventBridge 自定义事件总线是否附加了基于资源的策略。如果自定义事件总线策略没有附加基于资源的策略，则此规则为 NON_COMPLIANT。

标识符：CUSTOM_EVENTBUS_POLICY_ATTACHED

资源类型： AWS::Events::EventBus

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

cw-loggroup-retention-period-检查

检查 Amazon CloudWatch LogGroup 保留期是否设置为大于 365 天，或者是否设置为指定的保留期。如果保留期小于 `MinRetentionTime` 或者 365 天（如果指定此天数），则此规则为 NON_COMPLIANT。

> **Note**
>
> 如果日志组的保留设置为“永不过期”，则此规则将被标记为 COMPLIANT。

标识符：CW_LOGGROUP_RETENTION_PERIOD_CHECK

资源类型： AWS::Logs::LogGroup

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

LogGroupNames （可选），类型：CSV

要检查保留期的日志组名称的逗号分隔列表。

MinRetentionTime （可选），类型：int

指定以天为单位的保留时间。有效值为：
1、3、5、7、14、30、60、90、120、150、180、365、400、545、731、1827 和 3653。默认保留期为 365 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

datasync-task-logging-enabled

检查 Amazon DataSync 任务是否启用了 Amazon CloudWatch 日志记录。如果 Amazon DataSync 任务未启用 Amazon 日志记录，或者 CloudWatch 日志记录级别与您指定的日志级别不相等，则该规则不合规。

标识符：DATASYNC_TASK_LOGGING_ENABLED

资源类型： AWS::DataSync::Task

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

logLevel（可选），类型：字符串

日志记录级别的字符串值。有效值包括：“基本”和“转移”。如果未指定，则默认值为“基本”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dax-encryption-enabled

检查 Amazon DynamoDB Accelerator（DAX）集群是否已加密。如果 DAX 集群未加密，则此规则为 NON_COMPLIANT。

标识符：DAX_ENCRYPTION_ENABLED

资源类型： AWS::DAX::Cluster

触发器类型： 定期

Amazon Web Services 区域：仅在以下区域提供：欧洲地区（斯德哥尔摩）、中国（北京）、亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、欧洲地区（伦敦）、亚太地区（东京）、美国西部（俄勒冈州）、美国西部（北加利福尼亚）、亚太地区（新加坡）、亚太地区（悉尼）、欧洲（西班牙）、中国（宁夏）地区。

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

desired-instance-tenancy

检查 EC2 实例的 “租期” 值。还会检查 AMI IDs 是否指定从这些主机启动， AMIs 或者主机 IDs 是否在这些专用主机上启动。如果实例与列表中的主机和 AMI（如果指定）匹配，则此规则为 COMPLIANT。

标识符：DESIRED_INSTANCE_TENANCY

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

租期, 类型：字符串

实例的期望租期。有效值为 “专用”、“主机” 和 “默认”

imageId（可选）, 类型：CSV

该规则仅评估使用指定 IDs启动 AMIs 的实例。 IDs 用逗号分隔多个 AMI

hostId（可选）, 类型：CSV

要 IDs 在其上启动实例的 EC2 专用主机。 IDs 用逗号分隔多个主机

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

desired-instance-type

检查您的 EC2 实例是否属于特定的实例类型。如果参数列表中未指定 EC2 实例，则该规则不合规。有关支持的 EC2 实例类型的列表，请参阅 Linux 实例 EC2 用户指南中的实例类型。

标识符：DESIRED_INSTANCE_TYPE

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

instanceType, 类型：CSV

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

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dms-auto-minor-version-升级检查

检查 Amazon 数据库迁移服务 (Amazon DMS) 复制实例是否启用了自动次要版本升级。如果 Amazon DMS 复制实例未配置自动次要版本升级，则该规则不合规。

标识符：DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

资源类型： AWS::DMS::ReplicationInstance

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dms-endpoint-ssl-configured

检查 Amazon 数据库迁移服务 (Amazon DMS) 端点是否配置了 SSL 连接。如果 Amazon DMS 未配置 SSL 连接，则该规则不合规。

上下文：SSL/TLS 连接通过加密可在您的客户端和数据库实例集群之间移动的数据来提供一个安全层。使用服务器证书可验证是否正在与 Amazon RDS 数据库实例集群建立连接，从而额外提供一层安全保护。具体方法是，检查自动安装在您预置的所有数据库实例上的服务器证书。通过启用 SSL 连接 Amazon DMS，可以在迁移过程中保护数据的机密性。

要为配置 SSL 连接 Amazon DMS，请参阅 Amazon R SSL/TLS elational Database Service 用户指南中的使用加密与数据库实例或集群的连接。

标识符：DMS_ENDPOINT_SSL_CONFIGURED

资源类型： AWS::DMS::Endpoint

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dms-replication-instance-multi-az 已启用

检查 D Amazon atabase Migration Service (DMS) 复制实例是否配置了多个可用区。如果 DMS 复制实例未配置为使用多个可用区，则此规则为 NON_COMPLIANT。

标识符：DMS_REPLICATION_INSTANCE_MULTI_AZ_ENABLED

资源类型： AWS::DMS::ReplicationInstance

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dms-replication-not-public

检查 Amazon 数据库迁移服务 (Amazon DMS) 复制实例是否为公共实例。如果 PubliclyAccessible 字段设置为 true，则该规则不兼容。

标识符： DMS_REPLICATION_NOT_PUBLIC

资源类型： AWS::DMS::ReplicationInstance

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dms-replication-task-sourcedb-记录

检查是否为源数据库的 Amazon DMS 复制任务启用了有效的严重性级别的日志记录。如果未启用日志记录或源数据库的 DMS 复制任务的日志的严重性级别无效，则此规则为 NON_COMPLIANT。

标识符：DMS_REPLICATION_TASK_SOURCEDB_LOGGING

资源类型： AWS::DMS::ReplicationTask

触发器类型： 配置更改

Amazon Web Services 区域：除亚太地区（泰国）、亚太 Amazon 地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（大阪）、亚太地区（马来西亚）、（墨尔本）、（美国东部）、（美国西部）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里） Amazon GovCloud 、欧洲（西班牙苏黎世） Amazon GovCloud 、欧洲（苏黎世）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（苏黎世）、欧洲（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dms-replication-task-targetdb-记录

检查是否为目标数据库的 Amazon DMS 复制任务事件启用了有效的严重性级别的日志记录。如果未启用日志记录或目标数据库的复制任务日志记录的严重性级别无效，则此规则为 NON_COMPLIANT。

标识符：DMS_REPLICATION_TASK_TARGETDB_LOGGING

资源类型： AWS::DMS::ReplicationTask

触发器类型： 配置更改

Amazon Web Services 区域：除亚太地区（泰国）、亚太 Amazon 地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（大阪）、亚太地区（马来西亚）、（墨

尔本）、（美国东部）、（美国西部）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）Amazon GovCloud、欧洲（西班牙苏黎世）Amazon GovCloud、欧洲（苏黎世）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（苏黎世）、欧洲（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

docdb-cluster-encrypted-in-交通

检查与 Amazon DocumentDB 集群的连接是否配置为使用传输中加密。如果参数组不同步或者 TLS 参数设置为“disabled”或 `excludeTlsParameters` 中的值，则此规则为 NON_COMPLIANT。

标识符：DOCDB_CLUSTER_ENCRYPTED_IN_TRANSIT

资源类型： AWS::RDS::DBCluster

触发器类型： 定期

Amazon Web Services 区域：除欧洲（斯德哥尔摩）、中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（雅加达）、非洲（开普敦）、亚太地区（大阪）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、美国西部（加利福尼亚北部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）以外的所有支持区域，欧洲（苏黎世）地区

参数：

excludeTlsParameters （可选）, 类型：CSV

规则不会检查的 TLS 集群参数的逗号分隔列表。默认值：“disabled”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dynamodb-autoscaling-enabled

检查 Amazon DynamoDB 表或全局二级索引是否可以在启用 read/write 自动扩展的情况下使用按需模式或预配置模式处理容量。如果在未启用自动扩缩的情况下使用任一模式，则此规则为 NON_COMPLIANT

标识符：DYNAMODB_AUTOSCALING_ENABLED

资源类型： AWS::DynamoDB::Table

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

minProvisionedRead容量（可选）, 类型：int

应在自动扩缩组中对读取容量配置的最小单位数。

maxProvisionedRead容量（可选）, 类型：int

应在自动扩缩组中对读取容量配置的最大单位数。

targetReadUtilization （可选）, 类型：双精度

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。

minProvisionedWrite容量（可选）, 类型：int

应在自动扩缩组中对写入容量配置的最小单位数。

maxProvisionedWrite容量（可选）, 类型：int

应在自动扩缩组中对写入容量配置的最大单位数。

targetWriteUtilization （可选）, 类型：双精度

写入容量的目标使用率百分比。目标使用率以占用容量与预置容量的比值来表示。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dynamodb-in-backup-plan

检查备份计划中是否有 Amazon DynamoDB 表。 Amazon 如果任何备份计划中都没有 Amazon DynamoDB 表，则该规则不合规。 Amazon

标识符：DYNAMODB_IN_BACKUP_PLAN

资源类型： AWS::DynamoDB::Table

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

dynamodb-table-deletion-protection-已启用

检查 Amazon DynamoDB 表是否已将删除保护设置为已启用。如果该表的删除保护设置为禁用，则该规则为 NON_COMPLIANT。

标识符：DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

资源类型： AWS::DynamoDB::Table

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

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，此规则检查预置的吞吐量是否超过您的账户限制的阈值 (80%)。

标识符：DYNAMODB_THROUGHPUT_LIMIT_CHECK

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

账户RCUThreshold百分比（可选）, 类型：int, 默认值：80

为您的账户预配置的读取容量单位数的百分比。当达到此值时，规则将被标记为不合规。

账户WCUThreshold百分比（可选）, 类型：int, 默认值：80

为您的账户预配置的写入容量单位数的百分比。当达到此值时，规则将被标记为不合规。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ebs-in-backup-plan

检查 Backup 的备份计划中是否添加了亚马逊 Elastic Block Store (Amazon EBS) 卷。 Amazon 如果备份计划中未包含 Amazon EBS 卷，则此规则为 NON_COMPLIANT。

标识符：EBS_IN_BACKUP_PLAN

资源类型： AWS::EC2::Volume

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ebs-snapshot-block-public-访问

检查是否为某个 Amazon 地区的 Amazon EBS 快照启用了封锁公开访问功能。如果未为某个区域内所有公开共享 EBS 快照启用封禁公共访问权限，则该规则不合规。 Amazon

标识符：EBS_SNAPSHOT_BLOCK_PUBL

资源类型： AWS::EC2::SnapshotBlockPublicAccess

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ebs-snapshot-public-restorable-检查

检查 Amazon Elastic Block Store（Amazon EBS）是否不可公开还原。如果将一个或多个带 RestorableByUserIds 字段的快照设置为全部，即 Amazon EBS 快照是公开的，则该规则不合规。

标识符：EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

触发器类型： 定期

Amazon Web Services 区域: 除欧洲（西班牙） Amazon 区域之外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-ebs-encryption-by-default

检查 Amazon Elastic Block Store (EBS) 加密是否已默认启用。如果未启用加密，则规则为 NON_COMPLIANT。

标识符： EC2_EBS_ENCRYPTION _BY_DE

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-已enis-source-destination-check启用

检查用户 EC2 ENIs 管理是否启用了 source/destination 检查。如果禁用了 “lambda”、“aws_codestar_connections_managed”、“分支”、“efa”、“接口” 和 “quicksight” 的 source/destination 检查，则该规则不合规。 ENIs

标识符： EC2_ENIS_SOURCE_DESTINATION_ECK _ENABLED

资源类型： AWS::EC2::NetworkInterface

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-imdsv2-check

检查您的亚马逊弹性计算云 (Amazon EC2) 实例元数据版本是否配置了实例元数据服务版本 2 (IMDSv2)。如果设置为 可选，则该 HttpTokens 规则不兼容。

标识符： EC2_ IMDSV2 _CHECK

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-instance-launched-with-allowed-ami

检查正在运行或已停止的 EC2 实例是否使用符合允许 AMIs 标准的 Amazon 系统映像 (AMIs) 启动。如果 AMI 不符合允许标准且未禁用 “允许 AMIs AMIs ” 设置，则该规则为 “不合规”。

标识符： EC2_INSTANCE_LAUNCHED_WITH _ALLOUDE

资源类型： AWS::EC2::Instance

触发器类型：配置更改和定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

InstanceStateNameList （ 可选 ）, 类型：CSV

以逗号分隔的 Amazon EC2 实例状态列表，供规则检查。有效值为“running”和“stopped”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-管理instance-managed-by-systems器

> **Important**
>
> 对于此规则，规则标识符（EC2_INSTANCE_MANAGED_BY_SSM ）和规则名称（ec2--manager ）是不同的。instance-managed-by-systems

检查您的 Amazon EC2 实例是否由 Amazon Systems Manager 代理（SSM 代理）管理。如果实例正在运行且 SSM 代理已停止，或者 EC2 实例正在运行且 SSM 代理已终止，则 EC2 该规则不合规。

> **Note**
>
> 如果 EC2 实例已停止且 SSM 代理正在运行，则该规则不会返回 NON_COMPLIFT。

标识符： EC2_INSTANCE_MAN AGED_BY_SSM

资源类型： AWS::EC2::Instance， AWS::SSM::ManagedInstanceInventory

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-已加launch-templates-ebs-volume密

检查 Amazon EC2 启动模板是否为所有连接的 EBS 卷启用了加密。如果启动模板中配置的任何 EBS 卷的加密设置为 False，则该规则不合规。

标识符： EC2_LAUNCH_TEMPLATES _EBS_VOLUME_已加

资源类型： AWS::EC2::LaunchTemplate

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec launch-template-imdsv 2-2-check

检查当前设置的亚马逊 EC2 启动模板的默认版本是否要求新启动的实例使用亚马逊 EC2 实例元数据服务 (IMDSv2) 的 V2。如果未将 “元数据版本” 指定为 V2 () ，则该规则不兼容。IMDSv2

标识符： EC2_LAUNCH_TEM PLATE_ _CHEC IMDSV2

资源类型： AWS::EC2::LaunchTemplate

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部） Amazon GovCloud 、（美国西部） Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-launch-template-public-ip-已禁用

检查 Amazon EC2 启动模板是否设置为为网络接口分配公有 IP 地址。如果 EC2 启动模板的默认版本至少有 1 个网络接口且 “” 设置为 “trueAssociatePublicIpAddress” ，则该规则不兼容。

标识符： EC2_LAUNCH_TEMPLATE_PUBLIC _IP_禁用

资源类型： AWS::EC2::LaunchTemplate

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部） Amazon GovCloud 、（美国西部） Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

exemptedLaunchTemplates （可选），类型：CSV

以逗号分隔的豁免 EC2 启动模板列表 IDs ，允许将网络接口的 AssociatePublicIpAddress 值设置为 “true”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-managedinstance-applications-blacklisted

检查实例上是否未安装指定的任何应用程序。（可选）指定版本。较新的版本不会被列入拒绝名单。根据需要指定平台，仅针对运行该平台的实例应用规则。

标识符： EC2_MANAGEDINSTANCE_应用程序 _列入黑名单

资源类型： AWS::SSM::ManagedInstanceInventory

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

applicationNames, 类型：CSV

以逗号分隔的应用程序名称列表。（可选）指定附加有“:”的版本（例如，“Chrome: 0.5.3，FireFox”）。

> **Note**
>
> 应用程序名称必须完全匹配。例如，在 Linux 上使用 **`firefox`** 或在 Amazon Linux 上使用。**`firefox-compat`**此外，目前 Amazon Config 不支持 ApplicationN ames 参数的通配符（例如**`firefox*`**）。

platformType（可选），类型：字符串

平台类型（例如，“Linux”或“Windows”）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-managedinstance-applications-required

检查实例上是否安装了所有指定的应用程序。(可选）指定可接受的最低版本。您还可以指定平台，仅针对运行该平台的实例应用规则。

> **Note**
>
> 确保 SSM 代理正在 EC2 实例上运行，并且已创建用于收集应用程序软件清单的关联。如果未安装 SSM 代理或尚未创建或运行关联，则此规则将返回 `NOT_APPLICABLE`。

标识符： EC2_MANAGEDINSTA NCE_应用程序_必填

资源类型： AWS::SSM::ManagedInstanceInventory

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

applicationNames, 类型：CSV

以逗号分隔的应用程序名称列表。（可选）指定附加有“:”的版本（例如，“Chrome: 0.5.3，FireFox”）。

> **Note**
>
> 应用程序名称必须完全匹配。例如，在 Linux 上使用 **`firefox`** 或在 Amazon Linux 上使用。**`firefox-compat`**此外，目前 Amazon Config 不支持 ApplicationN ames 参数的通配符（例如**`firefox*`**）。

platformType（可选），类型：字符串

平台类型（例如，“Linux”或“Windows”）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-managedinstance-inventory-blacklisted

检查由 Amazon S EC2 ystems Manager 管理的实例是否配置为收集列入黑名单的库存类型。

标识符： EC2_MANAGEDINSTANCE_INVEN TORY_已列入

资源类型： AWS::SSM::ManagedInstanceInventory

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

inventoryNames, 类型：CSV

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

platformType（可选）, 类型：字符串

平台类型（例如，“Linux”）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-managedinstance-patch-compliance-status-check

在实例上安装补丁后，检查 Amazon Systems Manager 补丁合规性的合规状态是合规还是不兼容。如果字段状态为 COMPLIANT，则此规则为合规。

标识符： EC2_MANAGEDISTANCE_PATCH_COMPLIAN CE_STATUS

资源类型： AWS::SSM::PatchCompliance

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（大阪）、欧洲（米兰）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-managedinstance-platform-check

检查 EC2 托管实例是否具有所需的配置。

标识符： EC2_MANAGEDINSTA NCE_PLATFOR

资源类型： AWS::SSM::ManagedInstanceInventory

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

platformType, 类型：字符串

平台类型（例如，“Linux”）。

platformVersion（可选）, 类型：字符串

平台版本（例如，“2016.09”）。

agentVersion（可选）, 类型：字符串

代理版本（例如，“2.0.433.0”）。

platformName（可选）, 类型：字符串

平台版本（例如，“2016.09”）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-security-group-attached-to-eni

检查非默认安全组是否附加到亚马逊弹性计算云 (EC2) 实例或弹性网络接口 (ENIs)。如果安全组未与 EC2 实例或 ENI 关联，则该规则将返回 NON_COMPLIMENT。

标识符： EC2_SECURITY_GROUP_ATTACH ED_TO_ENI

资源类型： AWS::EC2::SecurityGroup

触发器类型： 配置更改

Amazon Web Services 区域：除中东（阿联酋）、加拿大西部（卡尔加里）地区以外的所有支持 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-stopped-instance

检查是否有亚马逊弹性计算云 (Amazon EC2) 实例停止的时间超过允许的天数。如果 Amazon EC2 实例的状态已停止超过允许的天数，或者无法确定时间，则该规则不合规。

标识符： EC2_STOPPED_IN STAN

资源类型： AWS::EC2::Instance

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

AllowedDays （可选），类型：int, 默认：30

在规则不合规之前，Amazon EC2 实例可以停止的天数。默认天数为 30。

> **Note**
>
> 所选天数必须少于配置的保留期，因为此规则依赖于收集的历史数据。有关历史数据保留的更多信息，请参阅删除 Amazon Config 数据。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecr-private-lifecycle-policy-已配置

检查私有 Amazon Elastic Container Registry（ECR）存储库是否配置了至少一项生命周期策略。如果没有为 ECR 私有存储库配置生命周期策略，则此规则为 NON_COMPLIANT。

标识符：ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

资源类型： AWS::ECR::Repository

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecr-private-tag-immutability-已启用

检查私有 Amazon Elastic Container Registry（ECR）存储库是否已启用标签不可变性。如果没有为私有 ECR 存储库启用标签不可变性，则此规则为 NON_COMPLIANT。

标识符：ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

资源类型： AWS::ECR::Repository

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecr-repository-cmk-encryption-已启用

检查 ECR 存储库是否使用客户管理的 KMS 密钥静态加密。如果使用 AES256 或默认 KMS 密钥 ('aws/ecr') 对存储库进行加密，则此规则不合规。

标识符：ECR_REPOSITORY_CMK_ENCRYPTION_ENABLED

资源类型： AWS::ECR::Repository

触发器类型： 配置更改

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）以外的所有支持区域

参数：

kmsKeyArns （可选），类型：CSV

以逗号分隔的 KMS 密钥列表 Amazon 资源名称 (ARNs)，用于加密 ECR 存储库。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-capacity-provider-termination-检查

检查包含 Auto Scaling 组的 Amazon ECS 容量提供商是否启用了托管终止保护。如果在 ECS 容量提供程序上禁用了托管终止保护，则此规则不合规。

标识符：ECS_CAPACITY_PROVIDER_PROVIDER_TERMIN

资源类型： AWS::ECS::CapacityProvider

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-containers-nonprivileged

检查 “定义” 容器定义中的特权参数是否设置为 “ ECSTasktrue”。如果特权参数为“true”，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_CONTAINERS_NONPRIVILEGED

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-containers-readonly-access

检查 Amazon Elastic Container Service（Amazon ECS）容器是否只能对其根文件系统进行只读访问。如果定义的容器定义中的 readonlyRootFilesystem 参数设置为 “f ECSTask alse”，则该规则不合规。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识：ECS_CONTAINERS_READONLY_ACCESS

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-container-insights-enabled

检查 Amazon Elastic Container Service 集群是否启用了容器洞察。如果未启用容器洞察，则此规则为 NON_COMPLIANT。

标识符：ECS_CONTAINER_INSIGHTS_ENABLED

资源类型： AWS::ECS::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-fargate-latest-platform-版本

检查 ECS Fargate 服务是否设置为最新平台版本。如果 Fargate PlatformVersion 的启动类型未设置为 LATEST，或者两者均未作为参数提供，则该规则 latestLinuxVersion 不`latestWindowsVersion`兼容。

标识符：ECS_FARGATE_LATEST_PLATFORM_VERSION

资源类型： AWS::ECS::Service

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

latestLinuxVersion （可选）, 类型：字符串

最新的 Linux 支持语义版本控制 (SemVer) 格式PlatformVersion的 “”。如果部署了 Fargate 并且已明确指定了 “PlatformVersion” 或将其用作 “” CodeDeploy ，则可能需要参数 DeploymentController

latestWindowsVersion （可选）, 类型：字符串

最新的 Windows 支持语义版本控制 (SemVer) 格式PlatformVersion的 “”。如果部署了 Fargate 并且已明确指定了 “PlatformVersion” 或将其用作 “” CodeDeploy ，则可能需要参数 DeploymentController

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-no-environment-secrets

检查机密是否作为容器环境变量传递。如果一个或多个环境变量键与“secretKeys”参数中列出的键匹配（不包括来自其他位置的环境变量，例如 Amazon S3），则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_NO_ENVIRONMENT_SECRETS

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

secretKeys, 类型：CSV

逗号分隔的键名列表，用于在任务定义中容器定义的环境变量中搜索。将删除多余的空格。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-task-definition-efs-已启用加密

检查带有 EFS 卷的 Amazon ECS 任务定义是否启用了传输中加密。如果 ECS 任务定义包含未启用传输加密的 EFS 卷，则该规则不合规。

标识符：ECS_TASK_DEFINITION_EFS_ENABLED

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-task-definition-linux-user-non-root

检查 Amazon ECS 任务定义的最新有效版本是否将 Linux 容器配置为以非 root 用户身份运行。如果指定了 root 用户或者任何容器都没有用户配置，则该规则不合规。

标识符：ECS_TASK_DEFINITION_LINUX_USER_NON_ROOT

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-task-definition-log-配置

检查是否在活动的 ECS 任务定义上设置了 logConfiguration。如果活动 ECSTask定义未定义日志配置资源，或者在至少一个容器定义中日志配置的值为空，则此规则不合规。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_TASK_DEFINITION_LOG_CONFIGURATION

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-task-definition-network-mode-not-host

检查 Amazon ECS 任务定义的最新活跃版本是否使用主机网络模式。如果 ECS 任务定义的最新活跃版本使用主机网络模式，则此规则为 NON_COMPLIANT。

标识符：ECS_TASK_DEFINITION_NETWORK_MODE_NOT_HOST

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-task-definition-pid-模式检查

检查 ECSTask定义是否配置为与其亚马逊弹性容器服务 (Amazon ECS) 容器共享主机的进程命名空间。如果 PidMode 参数设置为“host”，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_TASK_DEFINITION_PID_MODE_CHECK

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-task-definition-user-for-host-mode-check

检查具有主机网络模式的 Amazon ECS 任务定义在容器定义中是否具有特权或非根权限。如果任务定义的最新有效版本的 privileged=false（或为空）且 user=root（或为空），则该规则为 NON_COMPLIANT。

> **Important**
>
> 只需要满足一个条件即可使该规则返回 compliant
> 在以下任何情况下，该规则均为 COMPLIANT：
>
> - 如果网络模式未设置为主机，
> - 如果任务定义的最新当前修订版本的 privileged=true，
> - 如果任务定义的最新当前修订版本的用户不是根用户。
>
> 这意味着，只需要满足一个条件即可使该规则返回 compliant 要具体检查任务定义是否具有 priged=true 权限，请参阅。ecs-containers-nonprivileged要具体检查任务定义的用户是否不是 root，请参阅 ecs-task-definition-nonroot-user。

标识符：ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

SkipInactiveTaskDefinitions （可选），类型：布尔值

布尔值标志，用于不检查非活动的 Amazon EC2 任务定义。如果设置为 “true”，则该规则将不会评估非活动的 Amazon EC2 任务定义。如果设置为 “false”，则该规则将评估非活动亚马逊 EC2 任务定义的最新修订版。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ecs-task-definition-windows-user-non-admin

检查 Amazon ECS 任务定义的最新有效版本是否将 Windows 容器配置为以非管理员用户身份运行。如果指定了默认管理员用户或者任何容器都没有用户配置，则该规则为 NON_COMPLIMENT。

标识：ECS_TASK_DEFINITION_WINDOWS_USER_NON_ADMIN

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

efs-automatic-backups-enabled

检查 Amazon Elastic File System（Amazon EFS）文件系统是否启用了自动备份。如果 “BackupPolicy.Status” 设置为 “已禁用”，则该规则不兼容。

标识符：EFS_AUTOMATIC_BACKUPS_ENABLED

资源类型： AWS::EFS::FileSystem

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

efs-encrypted-check

检查是否将 Amazon Elastic File System (Amazon EFS) 配置为使用 Amazon Key Management Service (Amazon KMS) 加密文件数据。如果在 `DescribeFileSystems` 上将加密密钥设置为 false，或者 `DescribeFileSystems` 上的 `KmsKeyId` 密钥与 `KmsKeyId` 参数不匹配，则此规则为 NON_COMPLIANT。

标识符：EFS_ENCRYPTED_CHECK

资源类型： AWS::EFS::FileSystem

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

KmsKeyId （可选），类型：字符串

用于加密 EFS 文件系统的 KMS 密钥的 Amazon 资源名称（ARN）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

efs-filesystem-ct-encrypted

检查 Amazon Elastic File System (Amazon EFS) 是否使用 Amazon 密钥管理服务 (Amazon KMS) 对数据进行加密。如果文件系统未加密，则此规则为 NON_COMPLIANT。或者，您可以检查文件系统是否使用指定的 KMS 密钥进行加密。

标识符：EFS_FILESYSTEM_CT_ENCRYPTED

资源类型： AWS::EFS::FileSystem

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

kmsKeyArns （可选）, 类型：字符串

（可选）以逗号分隔的 Amazon KMS 密钥的 Amazon 资源名称列表 (ARNs)。如果提供，则该规则将检查指定的 KMS 密钥是否未加密 Amazon EFS 文件系统。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

efs-in-backup-plan

检查 Backup 的备份计划中是否添加了 Amazon Elastic File System (Amazon EFS) 文件系统。Amazon 如果备份计划中不包括 EFS 文件系统，则此规则为 NON_COMPLIANT。

标识符：EFS_IN_BACKUP_PLAN

资源类型： AWS::EFS::FileSystem

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

eip-attached

检查分配给 Amazon 账户的所有弹性 IP 地址是否都连接到 EC2 实例或正在使用的弹性网络接口。如果弹性 IP 地址的 “AssociationId” 为空，则该规则不合规。

> **Note**
>
> 评估发生后，可能需要最多 6 小时才能获得结果。

标识符：EIP_ATTACHED

资源类型： AWS::EC2::EIP

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 Amazon Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResourceEvaluationAPI 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
```

```
{
   "InstanceId": "my-instance-Id"
}
...
```

有关主动评估的更多信息，请参阅评估模式。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

eks-cluster-log-enabled

检查 Amazon Elastic Kubernetes Service（Amazon EKS）集群是否配置为启用日志记录。如果未启用 Amazon EKS 集群的日志记录，或者未启用上述日志类型的日志记录，则此规则为 NON_COMPLIANT。

标识符：EKS_CLUSTER_LOG_ENABLED

资源类型： AWS::EKS::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

logTypes（可选），类型：CSV

> 规则要检查的 EKS 集群控制面板日志类型的逗号分隔列表。有效值：“api”、“audit”、“authenticator”、“controllerManager”、“scheduler”

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

eks-cluster-supported-version

检查 Amazon Elastic Kubernetes Service（EKS）集群是否正在运行支持的 Kubernetes 版本。如果 EKS 集群正在运行不受支持的版本（小于参数“oldestVersionSupported”），则此规则为 NON_COMPLIANT。

标识符：EKS_CLUSTER_SUPPORTED_VERSION

资源类型： AWS::EKS::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

oldestVersionSupported, 类型：字符串

Amazon上支持的最旧版本的 Kubernetes 的值。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

eks-endpoint-no-public-访问

检查 Amazon Elastic Kubernetes Service（Amazon EKS）终端节点是否不可公开访问。如果终端节点可公开访问，则此规则为 NON_COMPLIANT。

标识符：EKS_ENDPOINT_NO_PUBLIC_ACCESS

资源类型： AWS::EKS::Cluster

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

eks-secrets-encrypted

检查 Amazon Elastic Kubernetes Service 集群是否配置为使用 (KMS) 密钥加密 Kubernetes 密钥。Amazon Key Management Service

- 如果 EKS 集群的 encryptionConfig 使用某个资源作为机密，则此规则为 COMPLIANT。
- 如果用于加密 EKS 机密的密钥与参数匹配，则此规则也为 COMPLIANT。
- 如果 EKS 集群没有 encryptionConfig 或 encryptionConfig 资源不包含机密，则此规则为 NON_COMPLIANT。
- 如果用于加密 EKS 机密的密钥与参数不匹配，则此规则也为 NON_COMPLIANT。

标识符：EKS_SECRETS_ENCRYPTED

资源类型： AWS::EKS::Cluster

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

kmsKeyArns （可选）, 类型：CSV

> KMS 密钥的 Amazon 资源名称（ARN）的逗号分隔列表，这些 ARN 应在 EKS 集群中用于加密的机密。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticache-auto-minor-version-升级检查

检查 Amazon ElastiCache 集群是否启用了自动次要版本升级。如果 ElastiCache 集群使用 Redis 或 Valkey 引擎，并且 “” 未设置为 “trueAutoMinorVersionUpgrade”，则该规则不合规。

标识符：ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

资源类型： AWS::ElastiCache::CacheCluster

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticache-redis-cluster-automatic-备份检查

检查 Amazon ElastiCache Redis 集群是否已开启自动备份。如果 Redis 集群的规则小于 SnapshotRetentionLimit 参数，则该规则不合规。 SnapshotRetentionPeriod 例如：如果参数为 15，则如果介于 0-15 之间，则规则不合规。 snapshotRetentionPeriod

标识符：ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

资源类型： AWS::ElastiCache::CacheCluster， AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

snapshotRetentionPeriod （可选）, 类型：int, 默认值：15

Redis 集群的最短快照保留期（以天为单位）。默认值为 15 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticache-repl-grp-auto-启用故障转移

检查 Amazon ElastiCache Redis 复制组是否启用了自动故障转移。如果 “” 未设置为 “已启用 AutomaticFailover”，则 ElastiCache 复制组的规则不兼容。

标识符：ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticache-repl-grp-encrypted-在休息时

检查 Amazon ElastiCache 复制组是否已 encryption-at-rest启用。如果禁用 “AtRestEncryptionEnabled” 或 KMS 密钥 ARN 与批准的 Arns 参数不匹配，则该 ElastiCache 复制组的规则不兼容。KMSKey

标识符：ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

批准的KMSKey身份证（可选），类型：CSV

经批准使用的 KMS 密钥列表 IDs ，以逗号分隔。 ElastiCache

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticache-repl-grp-encrypted在途中

检查 Amazon ElastiCache 复制组是否已 encryption-in-transit启用。如果 “” 设置为 “falseTransitEncryptionEnabled”，则 ElastiCache 复制组的规则不兼容。

标识符：ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticache-repl-grp-redis-已启用 auth

检查亚马逊 ElastiCache 复制组是否启用了 Redis 身份验证。如果 ElastiCache 复制组节点的 Redis 版本低于 6（版本 6+ 使用 Redis ACLs）并且 “AuthToken” 缺失或为空/空，则该复制组的规则不合规。

标识符：ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部） Amazon GovCloud 、（美国西部） Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticache-subnet-group-check

检查 Amazon ElastiCache 集群是否配置了自定义子网组。如果 ElastiCache 集群使用默认子网组，则该规则不合规。

标识符：ELASTICACHE_SUBNET_GROUP_CHECK

资源类型： AWS::ElastiCache::CacheCluster

触发器类型： 定期

Amazon Web Services 区域：除亚太地区（泰国）、亚太 Amazon 地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（大阪）、亚太地区（马来西亚）、（墨尔本）、（美国东部）、（美国西部）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里） Amazon GovCloud 、欧洲（西班牙苏黎世） Amazon GovCloud 、欧洲（苏

黎世）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（苏黎世）、欧洲（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticsearch-encrypted-at-rest

检查亚马逊 OpenSearch 服务（以前称为 Elasticsearch）域名是否启用了静态加密配置。如果未启用该 EncryptionAtRestOptions 字段，则该规则不兼容。

标识符：ELASTICSEARCH_ENCRYPTED_AT_REST

资源类型： AWS::Elasticsearch::Domain

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elasticsearch-in-vpc-only

检查亚马逊 OpenSearch 服务（以前称为 Elasticsearch）域名是否位于亚马逊虚拟私有云（亚马逊 VPC）中。如果 OpenSearch 服务域终端节点是公共的，则该规则不合规。

标识符：ELASTICSEARCH_IN_VPC_ONLY

资源类型： AWS::Elasticsearch::Domain

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elastic-beanstalk-managed-updates-已启用

检查 Amazon Elastic Beanstalk 环境中的托管平台更新是否已启用。如果 `ManagedActionsEnabled` 的值设置为 true，则此规则为 COMPLIANT。如果 `ManagedActionsEnabled` 的值设置为 false，或者提供了参数但其值与现有配置不匹配，则此规则为 NON_COMPLIANT。

标识符：ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

资源类型： AWS::ElasticBeanstalk::Environment

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（海得拉巴）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（苏黎世）以外的所有支持区域

参数：

UpdateLevel （可选）, 类型：字符串

表示更新级别是设置为“minor”版本更新还是“patch”版本更新。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elbv2-acm-certificate-required

检查应用程序负载均衡器和网络负载均衡器的侦听器是否配置为使用来自 Amazon Certificate Manager (ACM) 的证书。如果至少 1 个负载平衡器中有至少 1 个侦听器在配置时没有 ACM 证书或配置的证书与 ACM 证书不同，则此规则为 NON_COMPLIANT。

标识符： ELBV2_ACM_CERTIFICAT E_必填

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 定期

Amazon Web Services 区域：除亚太地区（泰国）、亚太 Amazon 地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（大阪）、亚太地区（马来西亚）、（墨尔本）、（美国东部）、（美国西部）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里） Amazon GovCloud 、欧洲（西班牙苏黎世） Amazon GovCloud 、欧洲（苏黎世）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（苏黎世）、欧洲（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）、欧洲（）区域

参数：

AcmCertificatesAllowed （可选）, 类型：CSV

以逗号分隔的证书列表 Amazon 资源名称 () ARNs。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elbv2-listener-encryption-in-transit

检查负载均衡器侦听器是否配置为 HTTPS 或 TLS 终止。如果侦听器未配置为 HTTPS 或 TLS 终止，则此规则为 NON_COMPLIANT。

标识符： ELBV2_LISTENER_ENCRYPTION _IN_TRAN

资源类型： AWS::ElasticLoadBalancingV2::Listener

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elbv2-multiple-az

检查 Elastic Load Balancer V2（应用程序、网络或网关负载均衡器）是否映射到多个可用区（AZs）。如果 Elastic Load Balancer V2 映射到小于 2，则该规则不合规。 AZs有关更多信息，请参阅应用程序负载均衡器的可用区。

标识符： ELBV2_MULTIPLE _AZ

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

minAvailabilityZones （可选）, 类型：int

预期的最小数量 AZs （介于 2 到 10 之间（含）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elb-acm-certificate-required

检查经典负载均衡器是否使用提供的 Amazon Certificate Manager 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

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

Amazon Web Services 区域：除非洲（开普敦）、亚太 Amazon 地区（大阪）、欧洲（米兰）、以色列（特拉维夫）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elb-custom-security-policy-ssl-check

检查您的经典负载均衡器 SSL 侦听器是否在使用自定义策略。此规则只适用于经典负载均衡器有 SSL 侦听器的情况。

标识符：ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

sslProtocolsAnd密码, 类型：CSV

逗号分隔的密码和协议列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

elb-predefined-security-policy-ssl 检查

检查您的经典负载均衡器 SSL 侦听器是否使用预定义的策略。如果 Classic Load Balanc HTTPS/SSLer 侦听器的策略不等于参数 “” `predefinedPolicyName` 的值，则该规则不合规。

标识符：ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

predefinedPolicyName, 类型：字符串

预定义策略的名称。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

emr-kerberos-enabled

检查 Amazon EMR 群集是否启用了 Kerberos。如果未将安全配置附加到群集或安全配置不满足指定的规则参数，则规则为 NON_COMPLIANT。

标识符：EMR_KERBEROS_ENABLED

资源类型： AWS::EMR::Cluster

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

TicketLifetimeInHours （ 可选 ）, 类型：int

群集 KDC 签发的 Kerberos 票证的有效期。

Realm（ 可选 ）, 类型：字符串

信任关系中另一领域的 Kerberos 领域名称。

Domain（ 可选 ）, 类型：字符串

信任关系中另一领域的域名。

AdminServer （ 可选 ）, 类型：字符串

信任关系的另一领域中的管理服务器的完全限定域名。

KdcServer （ 可选 ）, 类型：字符串

信任关系的另一领域中的 KDC 服务器的完全限定域名。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

emr-master-no-public-ip

检查 Amazon EMR 集群的主节点是否为公共节点。 IPs如果主节点具有公有 IP，则该规则为 NON_COMPLIANT。

> **Note**
>
> 此规则检查处于 RUNNING 或 WAITING 状态的集群。此规则要求您启用 `AWS::EC2::Instance` 资源类型的记录，以便进行准确的评估。

标识符：EMR_MASTER_NO_PUBLIC_IP

资源类型： AWS::EMR::Cluster， AWS::EC2::Instance

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

fms-webacl-resource-policy-检查

> **Note**
>
> 此规则目前正在逐步弃用中。建议不要直接使用它们。

检查 Web ACL 是否与应用程序负载均衡器、API Gateway 阶段或亚马逊 CloudFront 分配相关联。Amazon Firewall Manager 创建此规则时，FMS 策略所有者在 FMS 策略`WebACLId`中指定，并且可以选择启用补救。

标识符：FMS_WEBACL_RESOURCE_POLICY_CHECK

资源类型： AWS::CloudFront::Distribution、 AWS::ApiGateway::Stage、AWS::ElasticLoadBalancingV2::LoadBalancer、 AWS::WAFRegional::WebACL

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

网页 ACLId, 类型：字符串

Web o ACLId f Web ACL。

resourceTags（可选）, 类型：字符串

规则应与之关联的资源标签（ApplicationLoadBalancer ApiGatewayStage 和 CloudFront 分配）。（例如，{“tagKey1": [" tagValue1"]、“tagKey2"：[" tagValue2"、“tagValue3"]}）

excludeResourceTags（可选）, 类型：布尔值

如果为 true，则排除与 resourceTags 匹配的资源。

fmsManagedToken（可选）, 类型：字符串

Fi Amazon rewall Manager 在客户账户中创建规则时生成的令牌。 Amazon 当客户创建此规则时，Config 会忽略此参数。

fmsRemediationEnabled（可选）, 类型：布尔值

如果为 true，Fi Amazon rewall Manager 将根据 FMS 策略更新不合规的资源。 Amazon 当客户创建此规则时，Config 会忽略此参数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

fms-webacl-rulegroup-association-检查

> **Note**
>
> 此规则目前正在逐步弃用中。建议不要直接使用它们。

检查规则组是否与处于正确优先级的 Web ACL 关联。正确优先级由规则组在 ruleGroups 参数中的排名决定。 Amazon Firewall Manager 创建此规则时，它会分配最高优先级 0，然后是 1、2，依此类推。FMS 策略所有者在 FMS 策略中指定 `ruleGroups` 排名，并且可以选择启用补救功能。

标识符：FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

资源类型： AWS::WAF::WebACL， AWS::WAFRegional::WebACL

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

ruleGroups, 类型：字符串

以逗号分隔的 RuleGroupIds 和 WafOverrideAction 对列表。（例如， ruleGroupId-1: 无，2: COUNT） ruleGroupId

fmsManagedToken （可选）, 类型：字符串

Fi Amazon rewall Manager 在客户账户中创建规则时生成的令牌。 Amazon 当客户创建此规则时，Config 会忽略此参数。

fmsRemediationEnabled （可选）, 类型：布尔值

如果为 true，Fi Amazon rewall Manager 将根据 FMS 策略更新不合规的资源。 Amazon 当客户创建此规则时，Config 会忽略此参数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

fsx-ontap-deployment-type-检查

检查 Amazon FSx f NetApp or ONTAP 文件系统是否配置了某些部署类型。如果未使用您指定的部署类型配置 Amazon f FSx o NetApp r ONTAP 文件系统，则该规则不合规。

标识符：FSX_ONTAP_DEPLOYMENT_TYPE_CHECK

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）以外的所有支持区域

参数：

deploymentTypes, 类型：CSV

规则要检查的允许的部署类型的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

fsx-openzfs-deployment-type-检查

检查 Amazon fo FSx r OpenZFS 文件系统是否配置了某些部署类型。如果 FSx OpenZFS 文件系统未使用您指定的部署类型进行配置，则该规则不兼容。

标识符：FSX_OPENZFS_DEPLOYMENT_TYPE_CHECK

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）以外的所有支持区域

参数：

deploymentTypes, 类型：CSV

规则要检查的允许的部署类型的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

fsx-windows-deployment-type-检查

检查 Amazon f FSx or WINDOWS 文件系统是否配置了某些部署类型。如果 FSx 未使用您指定的部署类型配置 WINDOWS 文件系统，则该规则不兼容。

标识符：FSX_WINDOWS_DEPLOYMENT_TYPE_CHECK

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、欧洲（巴黎）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

deploymentTypes, 类型：CSV

规则要检查的允许的部署类型的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

glue-job-logging-enabled

检查 Amazon Glue 作业是否启用了日志记录。如果 G Amazon lue 任务未启用 Amazon CloudWatch 日志，则该规则不合规。

标识符：GLUE_JOB_LOGGING_ENABLED

资源类型： AWS::Glue::Job

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

glue-spark-job-supported-版本

检查 Amazon Glue Spark 作业是否在指定的最低支持的 Glue Amazon 版本上运行。如果 Glue Spark 作业未在您 Amazon 指定的最低支持的 Glu Amazon e 版本上运行，则该规则不兼容。

标识符：GLUE_SPARK_JOB_SUPPORTED_VERSION

资源类型： AWS::Glue::Job

触发器类型： 配置更改

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）以外的所有支持区域

参数：

minimumSupportedGlue版本, 类型：字符串

必须指定要检查的规则支持的最低 Amazon Glue 版本的字符串值。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

guardduty-enabled-centralized

检查您的 Amazon 账户和 Amazon 地区 GuardDuty 是否启用了亚马逊。如果您提供集中 Amazon 账户，则该规则将评估集中账户中的 GuardDuty 结果。启用后，该规则 GuardDuty 即为合规。

标识符：GUARDDUTY_ENABLED_CENTRALIZED

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

CentralMonitoringAccount （可选）, 类型：字符串

以逗号分隔的 Amazon 账户（12 位数）列表，允许集中管理亚马逊 GuardDuty 结果。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

guardduty-non-archived-findings

检查 Amazon 是否 GuardDuty 有未存档的调查结果。如果规则具有未存档的/参数，则 GuardDuty 该规则不low/medium/high severity findings older than the specified number in the daysLowSev/daysMediumSev合规。`daysHighSev`

标识符：GUARDDUTY_NON_ARCHIVED_FINDINGS

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

daysLowSev （可选）, 类型：int, 默认：30

允许 Amazon GuardDuty 低严重性调查结果处于非存档状态的天数。默认值为 30 天。

daysMediumSev （可选）, 类型：int, 默认：7

Amazon GuardDuty 中等严重性调查结果允许处于非存档状态的天数。默认值为 7 天。

daysHighSev （可选）, 类型：int, 默认：1

允许 Amazon GuardDuty 高严重性调查结果处于非存档状态的天数。默认值为 1 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-customer-policy-blocked-kms 动作

检查您创建的托管 Amazon 身份和访问管理 (IAM) Access Management 策略是否不允许对 Amazon 所有 KMS 密钥资源执行阻止 KMS 操作。如果托管 IAM 策略允许对所有 Amazon KMS 密钥执行任何阻止操作，则该规则不合规。

> **Note**
>
> 若要被视为非公有策略，IAM 策略必须仅向固定值授予访问权限。这意味着不包含通配符或以下 IAM 策略元素的值：变量。

标识符：IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

资源类型： AWS::IAM::Policy

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

blockedActionsPatterns, 类型：CSV

规则要检查的被阻止 KMS 操作模式的逗号分隔列表。如果 IAM 客户管理型策略允许通过通配符访问您指定的操作的所有资源，则此规则为 NON_COMPLIANT。

excludePermissionBoundary政策（可选）, 类型：布尔值

布尔标志，用于排除对用作权限边界的 IAM 策略的评估。如果设置为“true”，则此规则将不会在评估中包含权限边界。否则，当值设置为“false”时，系统会评估范围内的所有的 IAM 策略。默认值为“false”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-inline-policy-blocked-kms 动作

检查附加到您的 IAM 用户、角色和群组的内联策略是否不允许对所有 Amazon KMS 密钥执行阻止操作。如果允许对内联策略中的所有 Amazon KMS 密钥执行任何阻止操作，则该规则不合规。

标识符：IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

资源类型： AWS::IAM::Group、 AWS::IAM::Role、 AWS::IAM::User

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

blockedActionsPatterns, 类型：CSV

以逗号分隔的已屏蔽的 KMS 操作模式列表，例如， kms:*、 kms: Decrypt、*。 kms: ReEncrypt

excludeRoleByManagementAccount （可选）, 类型：布尔值

如果某个角色只能由组织管理账户代入，则将其排除在外。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-password-policy

检查针对 Amazon 身份和访问管理 (IAM) Management (IAM) 用户的账户密码策略是否符合参数中指示的指定要求。如果账户密码策略不符合指定要求，则此规则为 NON_COMPLIANT。

Important

规则参数的 `true` 和 `false` 值区分大小写。如果 `true` 未以小写形式提供，则将其视为 `false.`

Note

默认 IAM 密码策略的评估结果
使用默认 IAM 密码策略时，此规则会被标记为 NON_COMPLIANT。
托管规则和全局 IAM 资源类型
2022 年 2 月之前加入的全球 IAM 资源类型
（`AWS::IAM::GroupAWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）

只能在 2022 年 2 月之前可用的 Amazon Amazon Config 区域 Amazon Config 中进行记录。2022 年 2 月 Amazon Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 Amazon 资源 | 全球资源。
如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。
为避免不必要的评估，您应仅将报告全局 IAM 资源类型合规性的定期规则部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

标识符：IAM_PASSWORD_POLICY

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

RequireUppercaseCharacters （ 可选 ）, 类型：布尔值, 默认：True

密码中要求至少包含一个大写字符。

RequireLowercaseCharacters （ 可选 ）, 类型：布尔值, 默认：True

密码中要求至少包含一个小写字符。

RequireSymbols （ 可选 ）, 类型：布尔值, 默认：True

密码中要求至少包含一个符号。

RequireNumbers （ 可选 ）, 类型：布尔值, 默认：True

密码中要求至少包含一个数字。

MinimumPasswordLength （ 可选 ）, 类型：int, 默认值：14

密码最小长度。

PasswordReusePrevention （ 可选 ）, 类型：int, 默认值：24

允许重用前的密码数。

MaxPasswordAge （ 可选 ）, 类型：int, 默认值：90

密码到期前的天数。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-policy-blacklisted-check

检查每个 Amazon 身份和访问管理 (IAM) Access Management 资源，输入参数中的策略亚马逊资源名称 (ARN) 是否附加到该 IAM 资源。如果策略 ARN 已附加到 IAM 资源，则此规则为 NON_COMPLIANT。

标识符：IAM_POLICY_BLACKLISTED_CHECK

资源类型： AWS::IAM::User、 AWS::IAM::Group、 AWS::IAM::Role

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

policyArns, 类型：CSV, 默认：arn: aws: iam:: aws: policy/ AdministratorAccess

IAM 策略 ARN 的逗号分隔列表，不应将这些 ARN 附加到任何 IAM 实体。

exceptionList（可选）, 类型：CSV

以逗号分隔的资源类型列表和资源名称对列表。例如，users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3]。

> **Note**
>
> 在例外列表中，请指定资源的名称而不是完整 ARN。无效：`arn:aws:iam::444455556666:role/Admin`。有效：`Admin`

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-policy-in-use

检查 IAM 策略 ARN 是否附加到 IAM 用户，或包含一个或多个 IAM 用户的组，或包含一个或多个受信任实体的 IAM 角色。

> **Note**
>
> 托管规则和全局 IAM 资源类型
> 2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::GroupAWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 Amazon Amazon Config 区域 Amazon Config 中进行记录。2022 年 2 月 Amazon Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 Amazon 资源 | 全球资源。
> 如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。
> 为避免不必要的评估，您应仅将报告全局 IAM 资源类型合规性的定期规则部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

标识符： IAM_POLICY_IN_USE

资源类型： AWS::IAM::Policy

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

policyARN, 类型：字符串

要检查的 IAM 策略 ARN。

policyUsageType （可选）, 类型：字符串

指定是否希望将策略附加到 IAM 用户、组或角色。有效值为 IAM_USER、IAM_GROUP、IAM_ROLE 或 ANY。默认值为 ANY。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-policy-no-statements-with-admin-access

检查您创建的 Amazon 身份和访问管理 (IAM) 策略是否包含允许语句，这些语句授予对所有资源执行所有操作的权限。如果任何客户管理型 IAM 策略语句具有 "Effect": "Allow" with "Action": "*" over "Resource": "*"，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估客户管理型策略。此规则不评估内联策略或 Amazon 托管策略。有关差异的更多信息，请参阅《IAM 用户指南》中的托管式策略与内联策略。

以下策略为 NON_COMPLIANT：

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

以下策略为 COMPLIANT：

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
}
```

标识符：IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

资源类型： AWS::IAM::Policy

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

excludePermissionBoundary政策（可选），类型：布尔值

> 布尔标志，用于排除对用作权限边界的 IAM 策略的评估。如果设置为“true”，则此规则将不会在评估中包含权限边界。否则，当值设置为“false”时，系统会评估范围内的所有的 IAM 策略。默认值为“false”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-policy-no-statements-with-full-access

检查您创建的 Ident Amazon ity and Access Management (IAM) 策略是否授予对单个资源执行所有操作的权限。 Amazon 如果任何客户托管的 IAM 策略允许对至少 1 Amazon 项服务的完全访问权限，则该规则不合规。

上下文：根据最低权限原则，建议在授予 Amazon 服务权限时限制您的 IAM 策略中允许的操作。这种方法有助于确保您仅通过指定所需的确切操作来授予必要的权限，避免对服务使用不受限制的通配符，例如。`ec2:*`

在某些情况下，您可能希望允许使用相似前缀的多个操作，例如DescribeFlowLogs和DescribeAvailabilityZones。在这些情况下，您可以在通用前缀中添加带后缀的通配符（例如 `ec2:Describe*`）。分组相关操作有助于避免达到 IAM 策略大小限制。

如果您使用带有后缀通配符的前缀操作（例如 `ec2:Describe*`），则此规则将返回 COMPLIANT。仅当您使用不受限制的通配符（例如 `ec2:*`）时，此规则才会返回 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估客户管理型策略。此规则不评估内联策略或 Amazon 托管策略。有关差异的更多信息，请参阅《IAM 用户指南》中的托管式策略与内联策略。

标识符：IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

资源类型： AWS::IAM::Policy

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

excludePermissionBoundary政策（可选），类型：布尔值

> 布尔标志，用于排除对用作权限边界的 IAM 策略的评估。如果设置为“true”，则此规则将不会在评估中包含权限边界。否则，当值设置为“false”时，系统会评估范围内的所有的 IAM 策略。默认值为“false”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-root-access-key-检查

检查根用户访问密钥是否可用。如果用户访问密钥不存在，则此规则为 COMPLIANT。否则，将为 NON_COMPLIANT。

> **Note**
>
> 托管规则和全局 IAM 资源类型
> 2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::GroupAWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 Amazon Amazon Config 区域 Amazon Config 中进行记录。2022 年 2 月 Amazon Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 Amazon 资源 | 全球资源。
> 如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。

为避免不必要的评估，您应仅将报告全局 IAM 资源类型合规性的定期规则部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

标识符：IAM_ROOT_ACCESS_KEY_CHECK

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-user-mfa-enabled

检查 Amazon 身份和访问管理 (IAM) Access Management 用户是否启用了多重身份验证 (MFA)。如果没有为至少一个 IAM 用户启用 MFA，则此规则为 NON_COMPLIANT。

> **Note**
>
> 托管规则和全局 IAM 资源类型
> 2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::GroupAWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 Amazon Amazon Config 区域 Amazon Config 中进行记录。2022 年 2 月 Amazon Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 Amazon 资源 | 全球资源。
> 如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。

为避免不必要的评估，您应仅将报告全局 IAM 资源类型合规性的定期规则部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

标识符：IAM_USER_MFA_ENABLED

资源类型： AWS::IAM::User

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

iam-user-unused-credentials-检查

检查您的 Amazon Identity and Access Management (IAM) 用户是否拥有在您提供的指定天数内未使用的密码或有效访问密钥。如果存在最近未使用的非活动账户，则此规则为 NON_COMPLIANT。

Note

重新评估时间表
在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。
托管规则和全局 IAM 资源类型
2022 年 2 月之前加入的全球 IAM 资源类型
（`AWS::IAM::GroupAWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）
只能在 2022 年 2 月之前可用的 Amazon Amazon Config 区域 Amazon Config 中进行记录。2022 年 2 月 Amazon Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 Amazon 资源 | 全球资源。

如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。
为避免不必要的评估，您应仅将报告全局 IAM 资源类型合规性的定期规则部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

标识符：IAM_USER_UNUSED_CREDENTIALS_CHECK

资源类型： AWS::IAM::User

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

maxCredentialUsage年龄, 类型：int, 默认值：90

无法使用凭证的最大天数。默认值为 90 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

restricted-ssh

Important

对于此规则，规则标识符（INCOMING_SSH_DISABLED）和规则名称（restricted-ssh）是不同的。

检查安全组的传入 SSH 流量是否可访问。如果安全组中的传入 SSH 流量的 IP 地址受限（CIDR 而不是 0.0.0.0/0 或 ::/0），则此规则为 COMPLIANT。否则，将为 NON_COMPLIANT。

标识符：INCOMING_SSH_DISABLED

资源类型： AWS::EC2::SecurityGroup

触发器类型：配置更改和定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ec2-instances-in-vpc

> **Important**
> 对于此规则，规则标识符 (INSTANCES_IN_VPC) 和规则名称 (ec2-) 不同。instances-in-vpc

检查您的 EC2 实例是否属于虚拟私有云 (VPC)。或者，您可以指定要与您的实例关联的 VPC ID。

标识符：INSTANCES_IN_VPC

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

vpcId（可选）, 类型：字符串

包含这些 EC2 实例的 VPC ID。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

kinesis-stream-backup-retention-检查

检查 Amazon Kinesis Data Streams 是否将其数据记录留存期设置为特定的小时数。如果将属性 `RetentionPeriodHours` 设置为小于参数指定的值的值，则该规则不合规。

标识符：KINESIS_STREAM_BACKUP_RETENTION_CHECK

资源类型： AWS::Kinesis::Stream

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

minimumBackupRetention时期（可选），类型：字符串

应保留最少小时数的数据记录。有效值为 24 到 8760，默认值为 168。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

kinesis-stream-encrypted

检查 Amazon Kinesis 流是否使用服务器端加密进行加密。如果不存在 “StreamEncryption”，则该规则不符合 Kinesis 直播的规则。

背景：服务器端加密是 Amazon Kinesis Data Streams 中的一项功能，它使用 Amazon KMS 密钥在数据静止之前自动对其进行加密。数据在写入 Kinesis 流存储层之前加密，并在从存储检索到之后进行解密。因此，在 Kinesis Data Streams 服务中对数据进行静态加密。这有助于您满足监管要求并增强您数据的安全性。有关更多信息，请参阅 Amazon Kinesis Data Streams 数据保护。

标识符：KINESIS_STREAM_ENCRYPTED

资源类型： AWS::Kinesis::Stream

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

kms-cmk-not-scheduled-用于删除

检查 Amazon 密钥管理服务 (Amazon KMS) 密钥是否未计划在 Amazon KMS 中删除。如果计划删除 KMS 密钥，则此规则为 NON_COMPLIANT。

标识符：KMS_CMK_NOT_SCHEDULED_FOR_DELETION

资源类型： AWS::KMS::Key

触发器类型： 定期

Amazon Web Services 区域：除欧洲（米兰）、亚太 Amazon 地区（台北）地区以外的所有支持区域

参数：

kmsKeyIds （可选）, 类型：字符串

（可选）IDs 不计划删除的特定客户托管密钥列表，以逗号分隔。如果未指定任何密钥，则规则将检查所有密钥。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

kms-key-policy-no-公共访问

检查 Amazon KMS 密钥策略是否允许公开访问。如果 KMS 密钥政策允许公开访问 KMS 密钥，则此规则为 NON_COMPLIANT。

> **Note**
>
> 若要被视为非公有策略，KMS 密钥策略必须仅向固定值授予访问权限。这意味着不包含通配符或以下 IAM 策略元素的值：变量。

标识符：KMS_KEY_POLICY_NO_PUBLIC_ACCESS

资源类型： AWS::KMS::Key

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

mfa-enabled-for-iam-控制台访问权限

检查是否为 Amazon 所有使用控制台密码的 Amazon 身份和访问管理 (IAM) Access Management 用户启用了多重身份验证 (MFA)。如果已启用 MFA，则此规则为 COMPLIANT。

> **Note**
>
> 重新评估时间表
> 在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。
> 托管规则和全局 IAM 资源类型

2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::GroupAWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 Amazon Amazon Config 区域 Amazon Config 中进行记录。2022 年 2 月 Amazon Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 Amazon 资源 | 全球资源。
如果您至少在一个区域记录全局 IAM 资源类型，则报告全局 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域运行评估，即使您尚未在已添加定期规则的区域启用全局 IAM 资源类型的记录，也是如此。
为避免不必要的评估，您应仅将报告全局 IAM 资源类型合规性的定期规则部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 Amazon Config 托管规则列表。

标识符：MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

资源类型： AWS::IAM::User

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

mq-active-deployment-mode

检查为 Amazon MQ ActiveMQ 代理引擎配置的部署模式。如果使用的是默认的单实例代理模式，则此规则为 NON_COMPLIANT。

标识符：MQ_ACTIVE_DEPLOYMENT_MODE

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（海得拉巴）、亚太地区（海得拉巴）、亚太地区（马来西亚） Amazon GovCloud 、（美国东部） Amazon GovCloud 、（美国西部）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

mq-auto-minor-version-已启用升级

检查 Amazon MQ 代理是否启用了自动次要版本升级。如果未为 Amazon MQ 代理启用 AutoMinorVersionUpgrade “” 字段，则该规则不合规。

标识符：MQ_AUTO_MINOR_VERSION_EVERSION_UP

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（海得拉巴）、亚太地区（海得拉巴）、亚太地区（马来西亚） Amazon GovCloud 、（美国东部） Amazon GovCloud 、（美国西部）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

mq-rabbit-deployment-mode

检查为 Amazon MQ RabbitMQ 代理引擎配置的部署模式。如果使用的是默认的单实例代理模式，则此规则为 NON_COMPLIANT。

标识符：MQ_RABBIT_DEPLOYMENT_MODE

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（海得拉巴）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本） Amazon GovCloud 、（美国东部）、（美国西部） Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

msk-cluster-public-access-已禁用

检查是否在 Amazon MSK 集群上禁用了公有访问。如果 Amazon MSK 集群未禁用公开访问，则此规则为 NON_COMPLIANT。

标识符：MSK_CLUSTER_PUBLIC_ACCESS_DISABLED

资源类型： AWS::MSK::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

msk-enhanced-monitoring-enabled

检查是否为设置为 PER_TOPIC_PER_BROKER 或 PER_TOPIC_PER_PARTITION 的 Amazon MSK 集群启用了增强监控。如果启用了增强监控并设置为 DEFAULT 或 PER_BROKER，则此规则为 NON_COMPLIANT。

标识符：MSK_ENHANCED_MONITORING_ENABLED

资源类型： AWS::MSK::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

msk-in-cluster-node-需要-tls

检查 Amazon MSK 集群是否使用 HTTPS（TLS）对集群的代理节点进行传输中加密。如果为集群内代理节点连接启用了纯文本通信，则此规则为 NON_COMPLIANT。

标识符：MSK_IN_CLUSTER_NODE_REQUIRE_TLS

资源类型： AWS::MSK::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

msk-unrestricted-access-check

检查 Amazon MSK 集群是否已禁用未经身份验证的访问。如果 Amazon MSK 集群启用了未经身份验证的访问，则此规则为 NON_COMPLIANT。

标识符：MSK_UNRESTRICTED_ACCESS_CHECK

资源类型： AWS::MSK::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

multi-region-cloudtrail-enabled

> **Important**
>
> 对于此规则，规则标识符 (MULTI_REGION_CLOUD_TRAIL_ENABLED) 和规则名称 () 不同。multi-region-cloudtrail-enabled

检查是否至少有一个多区域 Amazon CloudTrail。如果跟踪与输入参数不匹配，则此规则为 NON_COMPLIANT。如果该`ExcludeManagementEventSources`字段不为空或配置为排除管理事件（例如 Amazon KMS 事件或 Amazon RDS 数据 API 事件），则 Amazon CloudTrail 该规则不合规。

标识符：MULTI_REGION_CLOUD_TRAIL_ENABLED

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

s3BucketName （可选）, 类型：字符串

用于 Amazon CloudTrail 向其传送日志文件的 Amazon S3 存储桶的名称。

snsTopicArn （可选）, 类型：字符串

用于通知的 Amazon SNS 主题 ARN Amazon CloudTrail 。

cloudWatchLogsLogGroupArn （可选）, 类型：字符串

Amazon CloudTrail 要向其发送数据的亚马逊 CloudWatch 日志组 ARN。

includeManagementEvents （可选）, 类型：布尔值

要包含 Amazon CloudTrail 的管理事件的事件选择器。

readWriteType （可选）, 类型：字符串

要记录的事件的类型。有效值为 ReadOnly、 WriteOnly 和 ALL。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

nacl-no-unrestricted-ssh-rdp

检查网络访问控制列表 (NACLs) 的 SSH/RDP 入口流量的默认端口是否不受限制。如果 NACL 入站条目允许端口 22 或 3389 使用源 TCP 或 UDP CIDR 块，则此规则为 NON_COMPLIANT。

标识符：NACL_NO_UNRESTRICTED_SSH_RDP

资源类型： AWS::EC2::NetworkAcl

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

netfw-subnet-change-protection-已启用

检查 Network Fire Amazon wall 是否启用了子网更改保护。如果子网变更保护未启用，则此规则为 NON_COMPLIANT。

标识符：NETFW_SUBNET_CHANGE_PROTECTION_ENABLED

资源类型： AWS::NetworkFirewall::Firewall

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

no-unrestricted-route-to-igw

检查路由表中是否有通向互联网网关（IGW）的公共路由。如果通向 IGW 的路由的目标 CIDR 块为“0.0.0.0/0”或“::/0”，或者目标 CIDR 块与规则参数不匹配，则此规则为 NON_COMPLIANT。

标识符：NO_UNRESTRICTED_ROUTE_TO_IGW

资源类型： AWS::EC2::RouteTable

触发器类型：配置更改和定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

routeTableIds （可选），类型：CSV

以逗号分隔的路由表列表，这些路由表可以 IDs 包含通往目标 CIDR 块为 '0.0.0.0/0' 或 ':: /0' 的 Internet Gateway 的路由。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

opensearch-update-check

检查 Amazon OpenSearch 服务版本更新是否可用但尚未安装。如果未安装最新的软件更新，则该 OpenSearch 域的规则不兼容。

标识符：OPENSEARCH_UPDATE_CHECK

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rabbit-mq-supported-version

检查 Amazon MQ RabbitMQ 代理是否在指定的最低支持引擎版本上运行。如果 RabbitMQ 代理未在您指定的最低支持引擎版本上运行，此规则为 NON_COMPLIANT。

标识符：RABBIT_MQ_SUPPORTED_VERSION

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（海得拉巴）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

supportedEngineVersion, 类型：字符串

用于检查 RabbitMQ 代理支持的最低引擎版本的规则的字符串值。RabbitMQ 代理使用语义版本控制规范：X.Y.Z。X 代表主要版本，Y 代表次要版本，Z 代表补丁版本。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-enhanced-monitoring-enabled

检查是否为 Amazon RDS 实例启用了增强监控。如果 RDS 实例的配置项中的“monitoringInterval”为“0”，或者“monitoringInterval”与规则参数值不匹配，则此规则为 NON_COMPLIANT。

标识符：RDS_ENHANCED_MONITORING_ENABLED

资源类型： AWS::RDS::DBInstance

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

monitoringInterval（可选），类型：int

一个整数值，表示为数据库实例收集增强监控指标时，点之间的秒数。有效值为 1、5、10、15、30 和 60。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 Amazon Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResourceEvaluationAPI 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

* 有关这些输入有效值的更多信息，请参阅 Amazon CloudFormation 用户指南中的MonitoringInterval和引擎。

有关主动评估的更多信息，请参阅评估模式。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-instance-subnet-igw-检查

检查 RDS 数据库实例是否部署在具有到互联网网关的路由的公有子网中。如果 RDS 数据库实例部署在公有子网中，则此规则为 NON_COMPLIANT

标识符：RDS_INSTANCE_SUBNET_IGW_CHECK

资源类型： AWS::RDS::DBInstance

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-in-backup-plan

检查 Amazon 备份计划中是否存在亚马逊关系数据库服务（Amazon RDS）数据库。如果任何 Amazon 备份计划中均未包含 Amazon RDS 数据库，则该规则不合规。

> **Note**
>
> 此规则仅适用于 Amazon Aurora 数据库实例。不支持数据库集群。

标识符：RDS_IN_BACKUP_PLAN

资源类型： AWS::RDS::DBInstance

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-logging-enabled

检查是否启用了 Amazon Relational Database Service（Amazon RDS）的相应日志。如果未启用任何日志记录，则此规则为 NON_COMPLIANT。

> **Note**
>
> 不处于“available”、“backing-up”、“storage-optimization”或“storage-full”状态的数据库实例评估为。NOT_APPLICABLE

标识符：RDS_LOGGING_ENABLED

资源类型： AWS::RDS::DBInstance

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

additionalLogs（可选），类型： StringMap

引擎名称和日志类型名称的逗号分隔列表。例如，"additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-mysql-instance-encrypted在途中

检查与 Amazon RDS for MySQL 数据库实例的连接是否配置为使用在传输中加密。如果关联的数据库参数组不同步或者 require_secure_transport 参数未设置为 1，则此规则为 NON_COMPLIANT。

> **Note**
>
> 如果 Amazon RDS 实例是 RDS 集群的一部分，则此规则将返回 `NOT_APPLICABLE`

标识符：RDS_MYSQL_INSTANCE_ENCRYPTED_IN_TRANSIT

资源类型： AWS::RDS::DBInstance

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-postgresql-logs-to-云观察

检查 Amazon PostgreSQL 数据库实例是否配置为向亚马逊日志发布日志。 CloudWatch 如果数据库实例未配置为向 Ama CloudWatch zon Logs 发布日志，则该规则不合规。

标识符：RDS_POSTGRESQL_LOGS_TO_CLOUDWATCH

资源类型： AWS::RDS::DBInstance

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

logTypes（可选），类型：CSV

要发布到 Logs 的日志类型列表，以逗号分隔。 CloudWatch 有效值为：“postgresql”、“upgrade”。默认值为“postgresql”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-postgres-instance-encrypted在途中

检查与 Amazon RDS PostgreSQL 数据库实例的连接是否配置为使用在传输中加密。如果关联的数据库参数组不同步或者 rds.force_ssl 参数未设置为 1，则此规则为 NON_COMPLIANT。

> **Note**
>
> 如果 Amazon RDS 实例是 RDS 集群的一部分，则此规则将返回 `NOT_APPLICABLE`

标识符：RDS_POSTGRES_INSTANCE_ENCRYPTED_IN_TRANSIT

资源类型： AWS::RDS::DBInstance

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-sqlserver-encrypted-in-交通

检查与 Amazon RDS SQL Server 数据库实例的连接是否配置为使用传输中加密。如果参数组的数据库参数 force_ssl 未设置为 1 或参数不是 “同步”，则该 ApplyStatus 规则不合规。

标识符：RDS_SQLSERVER_ENCRYPTED_IN_TRANSIT

资源类型： AWS::RDS::DBInstance

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

rds-sql-server-logs到云端观察

检查 Amazon SQL Server 数据库实例是否配置为向亚马逊日志发布 CloudWatch 日志。如果数据库实例未配置为向 Ama CloudWatch zon Logs 发布日志，则此规则不合规。

标识符：RDS_SQL_SERVER_LOGS_TO_CLOUDWATCH

资源类型： AWS::RDS::DBInstance

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

logTypes（可选），类型：CSV

LogTypes-（可选）：要发布到日志的日志类型列表，以逗号分隔。 CloudWatch 有效值为：“错误”、“代理”。默认值为“错误”、“代理”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-backup-enabled

检查集群是否启用了 Amazon Redshift 自动快照。如果 `automatedSnapshotRetentionPeriod` 的值大于 `MaxRetentionPeriod` 或小于，`MinRetentionPeriod`或者值为 0，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_BACKUP_ENABLED

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除墨西哥（中部）Amazon 区域之外的所有支持区域

参数：

MinRetentionPeriod （可选），类型：int

保留期的最小值。最小值为 1。

MaxRetentionPeriod （可选），类型：int

保留期的最大值。最大值为 35。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-cluster-configuration-check

检查 Amazon Redshift 集群是否具有指定的设置。如果 Amazon Redshift 集群未加密，或者是使用其他密钥加密的，或者集群未启用审核日志记录，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_CONFIGURATION_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除墨西哥（中部）Amazon 区域之外的所有支持区域

参数：

loggingEnabled, 类型：布尔值, 默认：True

已启用审核日志

clusterDbEncrypted, 类型：布尔值, 默认：True

数据库加密已启用

nodeTypes（可选）, 类型：CSV, 默认值：dc1.large

指定节点类型

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-cluster-maintenancesettings-check

检查 Amazon Redshift 集群是否具有指定的维护设置。如果禁用自动升级到主要版本，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除墨西哥（中部）Amazon 区域之外的所有支持区域

参数：

allowVersionUpgrade, 类型：布尔值, 默认：True

允许版本升级已启用。

preferredMaintenanceWindow （可选）, 类型：字符串

为集群计划的维护时段（例如，周一 09:30 - 周一 10:00）。

automatedSnapshotRetention时期（可选）, 类型：int, 默认：1

自动快照要被保留的天数。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 Amazon Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResourceEvaluationAPI 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
...
```

* 有关这些输入有效值的更多信息，请参阅《Amazon CloudFormation 用户指南》AllowVersionUpgrade中的AutomatedSnapshotRetentionPeriodPreferredMaintenanceWindow、和。

有关主动评估的更多信息，请参阅评估模式。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-cluster-multi-az-已启用

检查 Amazon Redshift 集群是否启用了多可用区部署。如果 Amazon Redshift 集群未启用多可用区部署，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_MULTI_AZ_ENABLED

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、墨西哥（中部）、美国西部（加利福尼亚北部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-cluster-subnet-group-多可用区

检查 Amazon Redshift 子网组是否包含来自多个可用区的子网。如果 Amazon Redshift 子网组不包含来自至少两个不同可用区的子网，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_SUBNET_GROUP_MULTI_AZ

资源类型： AWS::Redshift::ClusterSubnetGroup

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-default-admin-check

检查 Amazon Redshift 集群是否已将管理员用户名从其默认值更改为其他值。如果 Redshift 集群的管理员用户名设置为“awsuser”，或者用户名与参数中列出的用户名不匹配，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_DEFAULT_ADMIN_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

validAdminUser姓名（可选），类型：CSV

Redshift 集群要使用的管理员用户名的逗号分隔列表。注意：“awsuser”是默认值，不被接受。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-default-db-name-检查

检查 Redshift 集群是否已将其数据库名称从默认值更改为其他名称。如果 Redshift 集群的数据库名称设置为“dev”，或者提供了可选参数但数据库名称不匹配，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_DEFAULT_DB_NAME_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

validDatabaseNames （可选）, 类型：CSV

Redshift 集群的数据库名称的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-require-tls-ssl

检查 Amazon Redshift 集群是否需要 TLS/SSL 加密才能连接 SQL 客户端。如果任何 Amazon Redshift 集群的参数 require_SSL 未设置为 true，则此规则为 NON_COMPLIANT。

Identifier（标识符）：REDSHIFT_REQUIRE_TLS_SSL

资源类型： AWS::Redshift::Cluster， AWS::Redshift::ClusterParameterGroup

触发器类型： 配置更改

Amazon Web Services 区域：除墨西哥（中部）Amazon 区域之外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-serverless-default-admin-检查

检查 Amazon Redshift Serverless 命名空间是否已将管理员用户名从其默认值更改为其他值。如果 Redshift Serverless 命名空间的管理员用户名设置为 “admin”，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_SERVERLESS_DEFAULT_ADMIN_CHECK

资源类型： AWS::RedshiftServerless::Namespace

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、非洲（开普敦）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（马来西亚）、亚太地区（墨尔本）、欧洲（米兰）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-serverless-default-db-姓名检查

检查 Amazon Redshift Serverless 命名空间是否已将其数据库名称从默认值更改为其他名称。如果 Amazon Redshift Serverless 命名空间的数据库名称设置为 “dev”，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_SERVERLESS_DEFAULT_DB_NAME_CHECK

资源类型： AWS::RedshiftServerless::Namespace

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、非洲（开普敦）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（马来西亚）、亚太地区（墨尔本）、欧洲（米兰）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-serverless-namespace-cmk-加密

检查 Amazon Redshift 无服务器命名空间是否由客户托管的 KMS 密钥加密。 Amazon 如果命名空间未使用客户管理的密钥加密，则此规则为 NON_COMPLIANT。或者，您可以指定 KMS 密钥列表以供规则检查。

标识符：REDSHIFT_SERVERLESS_NAMESPACE_CMK_ENCRYPTION

资源类型： AWS::RedshiftServerless::Namespace

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、非洲（开普敦）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（马来西亚）、亚太地区（墨尔本）、欧洲（米兰）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

kmsKeyArns （可选）, 类型：CSV

> 以逗号分隔的客户托管密钥的 Amazon 资源名称 (ARNs) 列表，供规则检查。如果提供，并且 Amazon Redshift Serverless 命名空间未使用这些 KMS 密钥加密，则此规则为 NON_COMPLIANT。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-serverless-publish-logs到云端观察

检查 Amazon Redshift 无服务器命名空间是否配置为将以下日志发布到亚马逊日志。 CloudWatch 如果未将命名空间配置为向 Ama CloudWatch zon Logs 发布以下日志，则此规则不合规。

标识符：REDSHIFT_SERVERLESS_PUBLISH_LOGS_TO_CLOUDWATCH

资源类型： AWS::RedshiftServerless::Namespace

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、非洲（开普敦）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（马来西亚）、亚太地区（墨尔本）、欧洲（米兰）、（美国东部）、（美国西部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

logType（可选）, 类型：CSV

要发布到 Logs 的日志类型列表，以逗号分隔。 CloudWatch 有效值为“connectionlog”、“userlog”。默认值为“connectionlog”、“userlog”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

redshift-serverless-workgroup-routes-在 vpc 内

检查 Amazon Redshift Serverless 工作组是否通过 VPC 路由网络流量。如果工作组禁用“开启增强型 VPC 路由”，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_SERVERLESS_WORKGROUP_ROUTES_WITHIN_VPC

资源类型： AWS::RedshiftServerless::Workgroup

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（雅加达）、非洲（开普敦）、中东（阿联酋）、南美洲（圣保罗）、亚太地区（香港）、亚太地区（海得拉巴）、亚太地区（大阪）、亚太地区（马来西亚）、亚太地区（墨尔本）、欧洲（米兰）、（美国东部）、（美国西部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

required-tags

检查您的资源是否具有您指定的标签。例如，您可以检查您的 Amazon EC2 实例是否具有该`CostCenter`标签，同时还可以检查您的所有 RDS 实例是否都有一组密钥标签。用英文逗号分隔多个值。一次最多可以查看 6 个标签。

Amazon管理的 Amazon Systems Manager 自动化文档`AWS-SetRequiredTags`不能作为此规则的补救措施。您需要创建自己的自定义 Systems Manager 自动化文档以进行补救。

上下文： Amazon 允许您以标签的形式为 Amazon 资源分配元数据。每个标签都由一个键和一个可选值组成，用于存储有关资源的信息或保留在该资源上的数据。有关更多信息，请参阅制定标记策略。

您可以使用此规则来查找账户中未使用所需配置启动的资源，方法是指定哪些资源应具有标签以及每个标签的预期值。您也可以运行修复操作来修复标记错误。但是，此规则并不能防止您创建带有错误标签的资源。

> **Note**
>
> Amazon Config 不支持记录所有资源类型的关联标签。要验证是否在配置项目 (CI) 中 Amazon Config 记录了特定资源类型的标签，请执行以下操作：
>
> - 检查是否 Amazon Config 正确记录了资源的当前配置，不包括标签。
> - 当对资源进行更改时，该检查会 Amazon Config 刷新记录的配置。

标识符：REQUIRED_TAGS

资源类型： AWS::ACM::Certificate、 AWS::AutoScaling::AutoScalingGroup、、AWS::CloudFormation::Stack、 AWS::CodeBuild::Project、 AWS::DynamoDB::Table、AWS::EC2::CustomerGateway、 AWS::EC2::Instance、 AWS::EC2::InternetGateway、AWS::EC2::NetworkAcl、 AWS::EC2::NetworkInterface、 AWS::EC2::RouteTable、AWS::EC2::SecurityGroup、 AWS::EC2::Subnet、、 AWS::EC2::Volume、AWS::EC2::VPC、 AWS::EC2::VPNConnection、 AWS::EC2::VPNGateway、AWS::ElasticLoadBalancing::LoadBalancer、 AWS::ElasticLoadBalancingV2::LoadBalancer、

AWS::RDS::DBInstance、 AWS::RDS::DBSecurityGroup、 AWS::RDS::DBSnapshot、 AWS::RDS::DBSubnetGroup、 AWS::RDS::EventSubscription、、 AWS::Redshift::Cluster、 AWS::Redshift::ClusterParameterGroup、 AWS::Redshift::ClusterSecurityGroup、 AWS::Redshift::ClusterSnapshot、 AWS::Redshift::ClusterSubnetGroup、 AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

tag1Key, 类型：字符串, 默认： CostCenter

所需标签的键。

tag1Value（可选）, 类型：CSV

所需标签的可选值。用英文逗号分隔多个值。

tag2Key（可选）, 类型：字符串

第二个必需标签的键。

tag2Value（可选）, 类型：CSV

第二个所需标签的可选值。用英文逗号分隔多个值。

tag3Key（可选）, 类型：字符串

第三个所需标签的键。

tag3Value（可选）, 类型：CSV

第三个所需标签的可选值。用英文逗号分隔多个值。

tag4Key（可选）, 类型：字符串

第四个所需标签的键。

tag4Value（可选）, 类型：CSV

第四个所需标签的可选值。用英文逗号分隔多个值。

tag5Key（可选）, 类型：字符串

第五个所需标签的键。

tag5Value（可选）, 类型：CSV

第五个所需标签的可选值。用英文逗号分隔多个值。

tag6Key（可选），类型：字符串

第六个所需标签的键。

tag6Value（可选），类型：CSV

第六个所需标签的可选值。用英文逗号分隔多个值。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

restricted-common-ports

> **Important**
>
> 对于此规则，规则标识符 (RESTRICTED_INCOMING_TRAFFIC) 和规则名称 () 不同。restricted-common-ports

检查所用安全组是否不允许不受限制的传入传输控制协议（TCP）流量进入指定端口。在以下情况下，此规则为 COMPLIANT：

- 禁止所有 TCP 流量访问端口。
- 通过入站规则向 TCP 流量开放端口访问，其中来源要么是单个 IPv4 地址，要么是采用 CIDR 表示法的一系列地址，该 IPv4 地址不涵盖所有 IPv4 地址（“0.0.0.0/0”）。
- 通过入站规则向 TCP 流量开放端口访问，其中来源要么是单个 IPv6 地址，要么是采用 CIDR 表示法的一系列 IPv6 地址，该 IPv6 地址不涵盖所有地址（“:: /0)”）。

如果入站 TCP 连接的 IP 地址不限于指定端口，则此规则为 NON_COMPLIANT。

标识符：RESTRICTED_INCOMING_TRAFFIC

资源类型： AWS::EC2::SecurityGroup

触发器类型：配置更改和定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

blockedPort1（可选），类型：int, 默认值：20

已阻止的 TCP 端口号。默认值 20 对应于文件传输协议（FTP）数据传输。

blockedPort2（可选），类型：int, 默认值：21

已阻止的 TCP 端口号。默认值 21 对应于文件传输协议（FTP）命令控制。

blockedPort3（可选），类型：int, 默认值：3389

已阻止的 TCP 端口号。默认值 3389 对应于远程桌面协议（RDP）。

blockedPort4（可选），类型：int, 默认值：3306

已阻止的 TCP 端口号。默认值 3306 对应于 MySQL 协议。

blockedPort5（可选），类型：int, 默认值：4333

已阻止的 TCP 端口号。用于与您的环境相关的特定端口。

blockedPorts（可选），类型：CSV

被阻止的 TCP 端口号的逗号分隔列表。例如，20, 21, 3306, 3389。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

仅限 s3 access-point-in-vpc-

检查 Amazon S3 接入点是否不允许从互联网进行访问（NetworkOrigin 是 VPC）。如果 NetworkOrigin 是互联网，则该规则不兼容。

标识符：S3_ACCESS_POINT_IN_VPC_ONLY

资源类型： AWS::S3::AccessPoint

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3 access-point-public-access-方块

检查 Amazon S3 接入点是否启用了阻止公共访问设置。如果未为 S3 接入点启用阻止公共访问设置，则此规则为 NON_COMPLIANT。

标识符：S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

资源类型： AWS::S3::AccessPoint

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

excludedAccessPoints （可选）, 类型：CSV

允许的公共 Amazon S3 接入点列表（以逗号分隔）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3--account-level-public-access 区块-周期性

检查是否已在账户级别配置了所需的公有访问阻止设置。如果配置项与参数中的一个或多个设置（或默认设置）不匹配，则此规则为 NON_COMPLIANT。

标识符：S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

资源类型：AWS::::Account

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

IgnorePublicAcls （ 可选 ）, 类型：字符串

IgnorePublicAcls 是否强制执行，默认为 True

BlockPublicPolicy （ 可选 ）, 类型：字符串

BlockPublicPolicy 是否强制执行，默认为 True

BlockPublicAcls （ 可选 ）, 类型：字符串

BlockPublicAcls 是否强制执行，默认为 True

RestrictPublicBuckets （ 可选 ）, 类型：字符串

RestrictPublicBuckets 是否强制执行，默认为 True

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-acl-prohibited

检查亚马逊简单存储服务 (Amazon S3) Service Buckets 是否允许用户通过访问控制列表 () 获得权限。ACLs如果在 Amazon S3 存储桶中为用户访问进行了配置， ACLs 则该规则不合规。

标识符：S3_BUCKET_ACL_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-blacklisted-actions-prohibited

检查 Amazon Simple Storage Service (Amazon S3) 存储桶策略是否不允许其他账户的委托人对存储桶中的资源进行列入黑名单的存储桶级和对象级操作。 Amazon 例如，该规则会检查 Amazon S3 存储桶策略是否不允许其他 Amazon 账户`s3:DeleteObject`对存储桶中的任何对象执行任何`s3:GetBucket*`操作。如果 Amazon S3 存储桶策略允许任何列入黑名单的操作，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则只会检查 Principal 属性中的实体，不考虑策略中 Condition 属性下的任何条件

标识符：S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

blacklistedActionPattern, 类型：CSV

以逗号分隔的黑名单操作模式列表，例如 s3: GetBucket * 和 s3:。DeleteObject

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-已bucket-cross-region-replication启用

检查您是否已为 Amazon S3 存储桶启用 S3 跨区域复制功能。如果没有为跨区域复制启用复制规则，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_CROSS_REGION_REPLICATION_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-mfa-delete-enabled

检查 Amazon Simple Storage Service（Amazon S3）存储桶版本控制配置中是否启用了 MFA 删除。如果 MFA 删除未启用，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_MFA_DELETE_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-policy-grantee-check

检查 Amazon S3 存储桶授予的访问权限是否受到任何 Amazon 委托人、联合用户、服务委托人、IP 地址或您 VPCs 提供的限制。如果存储桶策略不存在，则此规则为 COMPLIANT。

例如，如果规则的输入参数为包含 111122223333 和 444455556666 这两个委托人的列表，并且存储桶策略指定仅 111122223333 能够访问存储桶，则此规则为 COMPLIANT。使用相同的输入参数：如果存储桶策略指定 111122223333 和 444455556666 可以访问存储桶，则此规则也为 COMPLIANT。

但是，如果存储桶策略指定 999900009999 可以访问存储桶，则此规则将为 NON_COMPLIANT。

> **Note**
>
> 如果存储桶策略包含多个语句，则将根据此规则评估存储桶策略中的每条语句。

标识符：S3_BUCKET_POLICY_GRANTEE_CHECK

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

awsPrincipals（可选），类型：CSV

以逗号分隔的委托人列表，例如 IAM 用户 ARNs、IAM 角色 ARNs和账户。 Amazon 您必须提供完整的 ARN 或使用部分匹配。例如，“arn: aws: iam:: role/*AccountID*” 或 “arn: aws: iam:: role/*” *role_name*。*AccountID*如果提供的值与存储桶策略中指定的主体 ARN 不完全匹配，则此规则为 NON_COMPLIANT。

servicePrincipals（可选），类型：CSV

逗号分隔的服务委托人列表，例如“cloudtrail.amazonaws.com, lambda.amazonaws.com”。

federatedUsers（可选），类型：CSV

Web 身份联合验证的身份提供商（如 Amazon Cognito 和 SAML 身份提供商）的逗号分隔列表。例如“cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider”。

ipAddresses（可选），类型：CSV

CIDR 格式的 IP 地址的逗号分隔列表，例如“10.0.0.1, 192.168.1.0/24, 2001:db8::/32”。

vpcIds（可选），类型：CSV

以逗号分隔的亚马逊虚拟私有云（亚马逊 VPC）列表，例如 'vpc-1234abc0 IDs、vpc-ab1234c0'。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-policy-not-more-宽容

验证您的 Amazon Simple Storage Service 存储桶策略是否不允许您提供的控制 Amazon S3 存储桶策略之外的其他账户间权限。

> **Note**
>
> 如果您提供了无效的参数值，则将看到以下错误：controlPolicy 参数的值必须是 Amazon S3 存储桶策略。

标识符：S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

controlPolicy, 类型：字符串

定义您的 S3 存储桶的权限上限的 Amazon S3 存储桶策略。此策略的最大长度为 1024 个字符。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-public-read-prohibited

检查您的 Amazon S3 存储桶是否不允许公有读取访问。该规则将检查“阻止公有访问”设置、存储桶策略和存储桶访问控制列表（ACL）。

当满足以下两个条件时，该规则也合规：

- “阻止公有访问”设置限制公有策略，或者存储桶策略不允许公有读取访问。
- “阻止公共访问” 设置限制了公共访问权限， ACLs 或者存储桶 ACL 不允许公共读取权限。

在以下情况下，该规则不合规：

- 如果 “阻止公共访问” 设置不限制公共策略，则 Amazon Config 评估该策略是否允许公共读取权限。如果策略允许公有读取访问，则该规则不合规。
- 如果 “阻止公共访问” 设置不限制公共存储桶 ACLs，则 Amazon Config 评估存储桶 ACL 是否允许公共读取权限。如果存储桶 ACL 允许公有读取访问，则规则将不合规。

> **Note**
>
> 若要被视为非公有策略，S3 存储桶策略必须仅向固定值授予访问权限。这意味着不包含通配符或以下 IAM 策略元素的值：变量。

标识符：S3_BUCKET_PUBLIC_READ_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型：配置更改和定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-public-write-prohibited

检查您的 Amazon S3 存储桶是否允许公有写入访问。该规则将检查“阻止公有访问”设置、存储桶策略和存储桶访问控制列表（ACL）。

当满足以下两个条件时，该规则也合规：

- “阻止公有访问”设置限制公有策略，或者存储桶策略不允许公有写入访问。
- “阻止公共访问” 设置限制公共访问权限 ACLs 或存储桶 ACL 不允许公共写入权限。

在以下情况下，该规则不合规：

- 如果 “阻止公共访问” 设置不限制公共策略，则 Amazon Config 评估该策略是否允许公共写入权限。如果策略允许公有写入访问，则该规则不合规。
- 如果 “阻止公共访问” 设置不限制公共存储桶 ACLs，则 Amazon Config 评估存储桶 ACL 是否允许公共写入权限。如果存储桶 ACL 允许公有写入访问，则规则将不合规。

> **Note**
>
> 此规则不评估账户级别阻止公有访问权限的更改。要检查所需的公共访问屏蔽设置是否是从账户级别配置的，请参阅 s3-bloc account-level-public-access ks 和 s3-blocks-p er account-level-public-accessicial。

> **Note**
>
> 若要被视为非公有策略，S3 存储桶策略必须仅向固定值授予访问权限。这意味着不包含通配符或以下 IAM 策略元素的值：变量。

标识符：S3_BUCKET_PUBLIC_WRITE_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型：配置更改和定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-replication-enabled

检查 S3 存储桶是否启用了复制规则。如果 S3 存储桶没有复制规则或复制规则未启用，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_REPLICATION_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

ReplicationType （ 可选 ）, 类型：字符串

> 接受的值：“CROSS-REGION”和“SAME-REGION”。对规则输入“CROSS-REGION”，以检查所有存储桶是否仅启用了跨区域复制。对规则输入“SAME-REGION”，以检查所有存储桶是否仅启用了同区域复制。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-已bucket-server-side-encryption启用

检查您的 Amazon S3 存储桶是否已启用 Amazon S3 默认加密，或 Amazon S3 存储桶策略是否显式拒绝未进行服务器端加密（使用 AES-256 或 Amazon Key Management Service ）的 `put-object` 请求。如果您的 Amazon S3 存储桶默认未加密，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-bucket-ssl-requests-only

检查 S3 存储桶是否具有需要请求使用 SSL/TLS 的策略。如果任何 S3 存储桶具有允许 HTTP 请求的策略，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_SSL_REQUESTS_ONLY

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-default-encryption-kms

检查 S3 存储桶是否使用 Amazon 密钥管理服务 (Amazon KMS) 加密。如果 S3 存储桶未使用 Amazon KMS 密钥加密，则该规则不合规。

Identifier (标识符)：S3_DEFAULT_ENCRYPTION_KMS

资源类型： AWS::S3::Bucket， AWS::KMS::Key

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

kmsKeyArns （可选）, 类型：CSV

ARNs 允许加密 Amazon S3 存储桶的 Amazon KMS 密钥列表，以逗号分隔。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-event-notifications-enabled

检查 S3 存储桶上是否启用了 Amazon S3 事件通知。如果存储桶上未设置 S3 事件通知，或者事件类型或目标与 `eventTypes` 和 destinationArn 参数不匹配，则此规则为 NON_COMPLIANT。

标识符：S3_EVENT_NOTIFICATIONS_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、亚太地区（雅加达）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

destinationArn（可选）, 类型：字符串

事件通知目标的亚马逊资源名称 (ARN)（亚马逊 SNS 主题、 Amazon Lambda、亚马逊 SQS 队列）。

eventTypes（可选），类型：CSV

首选 Amazon S3 事件类型的逗号分隔列表

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-lifecycle-policy-check

检查是否为 Amazon Simple Storage Service（Amazon S3）存储桶配置了生命周期规则。如果没有有效的生命周期配置规则，或者配置与参数值不匹配，则此规则为 NON_COMPLIANT。

标识符：S3_LIFECYCLE_POLICY_CHECK

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

targetTransitionDays （可选），类型：int

对象在创建后过渡到指定存储类的天数（例如 30 天）。

targetExpirationDays （可选），类型：int

对象创建后删除对象的天数（例如，395 天）。

targetTransitionStorage班级（可选），类型：字符串

目标存储类类型。例如，Amazon S3 Standard-Infrequent Access（S3 Standard-IA）。有关更多信息，请参阅了解和管理 Amazon S3 存储类别。

targetPrefix（可选），类型：字符串

用于标识一个或多个对象的 Amazon S3 对象前缀。

bucketNames（可选），类型：CSV

启用生命周期策略的 Amazon S3 存储桶名称的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

s3-version-lifecycle-policy-check

检查启用了 Amazon Simple Storage Service（Amazon S3）版本的存储桶是否配置了生命周期策略。如果未启用 Amazon S3 生命周期策略，则此规则为 NON_COMPLIANT。

标识符：S3_VERSION_LIFECYCLE_POLICY_CHECK

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

bucketNames（可选），类型：CSV

启用生命周期策略的 Amazon S3 存储桶名称的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sagemaker-endpoint-configuration-kms-密钥已配置

检查是否为亚马逊 SageMaker 终端节点配置配置了密 Amazon 钥管理服务 (Amazon KMS) 密钥。如果未为 Amazon SageMaker 终端节点配置指定 KmsKeyId “”，则该规则不合规。

标识符：SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

资源类型： AWS::SageMaker::EndpointConfig

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

kmsKeyArns （可选），类型：字符串

Amazon SageMaker 终端节点配置 ARNs 允许的特定 Amazon KMS 密钥列表，以逗号分隔。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sagemaker-notebook-instance-inside-vpc

检查 Amazon SageMaker 笔记本实例是在 VPC 内启动的，还是在已批准的子网列表中启动。如果笔记本实例不是在 VPC 内启动，或者其子网 ID 未包含在参数列表中，则此规则为 NON_COMPLIANT。

标识符：SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部） Amazon GovCloud 、（美国西部） Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

SubnetIds （可选），类型：CSV

可以启动笔记本实例的子网列表 IDs ，以逗号分隔。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sagemaker-notebook-instance-kms-密钥已配置

检查是否为 Amazon SageMaker 笔记本实例配置了密 Amazon 钥管理服务 (Amazon KMS) 密钥。如果未为 SageMaker 笔记本实例指定 “KmsKeyId”，则该规则不兼容。

标识符：SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

kmsKeyArns （可选）, 类型：字符串

Amazon SageMaker 笔记本实例 ARNs 允许的 Amazon KMS 密钥列表，以逗号分隔。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sagemaker-notebook-instance-platform-版本

检查 Sagemaker 笔记本实例是否配置为使用支持的平台标识符版本。如果笔记本实例未使用参数中指定的受支持平台标识符版本，则此规则为 NON_COMPLIANT。

标识符：SAGEMAKER_NOTEBOOK_INSTANCE_PLATFORM_VERSION

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 定期

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）以外的所有支持区域

参数：

supportedPlatformIdentifier版本, 类型：CSV

规则要检查的受支持平台标识符版本的逗号分隔列表。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sagemaker-notebook-instance-root-访问检查

检查是否为亚马逊 SageMaker 笔记本实例启用了 Amazon SageMaker RootAccess 设置。如果将 Amazon SageMaker 笔记本实例的 RootAccess 设置设置为 “已启用”，则该规则不合规。

标识符：SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部） Amazon GovCloud 、（美国西部） Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sagemaker-notebook-no-direct-互联网接入

检查 Amazon SageMaker 笔记本实例是否禁用了直接互联网接入。如果 SageMaker 笔记本实例支持互联网，则该规则不兼容。

标识符：SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

secretsmanager-rotation-enabled-check

检查 S Amazon ecrets Manager 密钥是否启用了轮换。此外，该规则还检查可选 `maximumAllowedRotationFrequency` 参数。如果指定了参数，则密钥的轮换频率与允许的最大频率进行比较。如果密钥未计划轮换，则此规则为 NON_COMPLIANT。如果旋转频率高于 Frequency 参数中指定的数字，则该规则也是 NON_Complift。 maximumAllowedRotation

> **Note**
>
> 在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。

标识符： SECRETSMANAGER_ROTATION_ENABLED_CHECK

资源类型： AWS::SecretsManager::Secret

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

maximumAllowedRotationFrequencyInHours （可选）, 类型：int

机密允许的最大轮换频率（以小时为单位）。

maximumAllowedRotation频率（可选）, 类型：int

密钥允许的最大轮换频率（以天为单位）。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

secretsmanager-secret-periodic-rotation

检查 S Amazon ecrets Manager 的密钥是否在过去指定的天数内被轮换。如果密钥的轮换天数未超过maxDaysSince轮换天数，则该规则为 NON_COMPLIMENT。默认值为 90 天。

标识符：SECRETSMANAGER_SECRET_PERIODIC_ROTATION

资源类型： AWS::SecretsManager::Secret

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

maxDaysSince旋转（可选），类型：int

机密可以保持不变的最大天数。默认值为 90 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

secretsmanager-secret-unused

检查 S Amazon ecrets Manager 密钥是否在指定的天数内被访问。如果在 “unusedForDays” 天数内未访问密钥，则该规则不合规。默认值为 90 天。

背景：建议定期删除未使用的机密。未使用的机密可能会被不再需要访问这些机密的前用户滥用。此外，获得机密访问权的用户越多，有人滥用机密或将访问权授予未经授权实体的可能性也就越大。删除未使用的机密有助于撤消不再需要机密的用户的机密访问权限，还可以降低您使用 Amazon Secrets Manager的成本。

标识符：SECRETSMANAGER_SECRET_UNUSED

资源类型： AWS::SecretsManager::Secret

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

unusedForDays （ 可选 ）, 类型：int

机密可以保持未使用状态的天数。默认值为 90 天。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

secretsmanager-using-cmk

检查中的 Amazon Secrets Manager 所有密钥是否使用 Amazon 托管式密钥 (`aws/secretsmanager`) 或在 () 中 Amazon Key Management Service 创建的客户托管密钥进行加密。Amazon KMS如果使用客户管理型密钥来加密机密，则此规则为 COMPLIANT。如果使用 `aws/secretsmanager` 加密机密，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则无法访问跨账户客户管理型密钥，因此在使用跨账户密钥时，会将机密评估为 NON_COMPLIANT。

标识符：SECRETSMANAGER_USING_CMK

资源类型： AWS::SecretsManager::Secret

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

kmsKeyArns （ 可选 ）, 类型：CSV

以逗号分隔的 KMS 密钥列表 Amazon 资源名称 (ARNs)，用于检查密钥是否用于加密。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

securityhub-enabled

检查 Amazon 账户是否启用了 Sec Amazon urity Hub。如果未启用 Sec Amazon urity Hub，则该规则不合规。

Identifier（标识符）：SECURITYHUB_ENABLED

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

security-account-information-provided

检查您是否为 Amazon 账户联系人提供了安全联系人信息。如果未提供账户内的安全联系人信息，则此规则为 NON_COMPLIANT。

标识符：SECURITY_ACCOUNT_INFORMATION_PROVIDED

资源类型：AWS::::Account

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

service-vpc-endpoint-enabled

检查是否已为每个 Amazon Virtual Private Cloud（Amazon VPC）创建规则参数中提供的服务的服务终端节点。如果 Amazon VPC 没有为该服务创建 VPC 终端节点，则此规则为 NON_COMPLIANT。

标识符：SERVICE_VPC_ENDPOINT_ENABLED

资源类型： AWS::EC2::VPC

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

serviceName, 类型：字符串

> 服务的短名称或后缀。注意：要获取可用服务名称列表或有效后缀列表，请使用 DescribeVpcEndpointServices。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sns-topic-message-delivery-启用通知

检查是否已启用 Amazon Simple Notification Service（SNS）日志记录，以记录发送到端点主题的通知消息的传送状态。如果未启用消息的传送状态通知，则此规则为 NON_COMPLIANT。

标识符：SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

资源类型： AWS::SNS::Topic

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sns-topic-no-public-访问

检查 SNS 主题访问策略是否允许公开访问。如果 SNS 主题访问策略允许公开访问，则此规则为 NON_COMPLIANT。

> **Note**
>
> 若要被视为非公有策略，SNS 策略必须仅向固定值授予访问权限。这意味着不包含通配符或以下 IAM 策略元素的值：变量。

标识符：SNS_TOPIC_NO_PUBLIC_ACCESS

资源类型： AWS::SNS::Topic

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sqs-queue-dlq-check

检查 Amazon Simple Queue Service（Amazon SQS）队列是否配置为使用死信队列（DLQ）。如果 Amazon SQS 队列没有任何使用 DLQ 的配置，则此规则为 NON_COMPLIANT。

标识符：SQS_QUEUE_DLQ_CHECK

资源类型： AWS::SQS::Queue

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sqs-queue-no-public-访问

检查 SQS 队列访问策略是否允许公开访问。如果 SQS 队列访问策略允许公开访问，则此规则为 NON_COMPLIANT。

> **Note**
>
> 若要被视为非公有策略，SQS 策略必须仅向固定值授予访问权限。这意味着不包含通配符或以下 IAM 策略元素的值：变量。

标识符：SQS_QUEUE_NO_PUBLIC_ACCESS

资源类型： AWS::SQS::Queue

触发器类型： 配置更改

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲以外的所有支持区域（苏黎世）地区

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

sqs-queue-policy-full-访问检查

检查 SQS 队列访问策略是否允许完全访问。如果 SQS 策略在“操作”中包含“SQS: *”，且“效果”为“允许”，则此规则为 NON_COMPLIANT。

标识符：SQS_QUEUE_POLICY_FULL_ACCESS_CHECK

资源类型： AWS::SQS::Queue

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ssm-automation-block-public-共享

检查 Amazon Systems Manager 文档是否启用了屏蔽公共共享。如果 Systems Manager Documents 已禁用块公开共享，则此规则为 NON_COMPLIANT。

标识符：SSM_AUTOMATION_BLOCK_PUBLIC_SHARING

资源类型：AWS::::Account

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ssm-automation-logging-enabled

检查 Amazon Systems Manager Automation 是否启用了亚马逊 CloudWatch 日志记录。如果 Systems Manager Automation 未 CloudWatch 启用日志记录，则该规则将返回 “不合规”。

标识符：SSM_AUTOMATION_LOGGING_ENABLED

资源类型：AWS::::Account

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、墨西哥（中部）、亚太地区（台北）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

ssm-document-not-public

检查该账户拥有的 Amazon Systems Manager 文档是否公开。如果所有者为“Self”的 Systems Manager 文档是公有的，则此规则为 NON_COMPLIANT。

标识符：SSM_DOCUMENT_NOT_PUBLIC

资源类型： AWS::SSM::Document

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（台北）区域之外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

step-functions-state-machine-启用日志功能

检查 Ste Amazon p Functions 计算机是否启用了日志功能。如果状态机未启用日志记录，或日志记录配置未达到提供的最低级别，则此规则为 NON_COMPLIANT。

标识符：STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

资源类型： AWS::StepFunctions::StateMachine

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、亚太地区（墨尔本）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

cloudWatchLogGroupArns （可选）, 类型：CSV

Amazon Lo CloudWatch gs 日志组的亚马逊资源名称 (ARNs) 列表，以逗号分隔。此规则检查是否为状态机日志配置了指定的日志组。

logLevel（可选）, 类型：字符串

状态机的最低日志级别。有效值包括：ALL、ERROR、FATAL。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

subnet-auto-assign-public-ip 已禁用

检查 Amazon Virtual Private Cloud（Amazon VPC）子网是否配置为自动为在子网中启动的实例分配公有 IP 地址。如果子网不自动分配公共地址 IPv4 或 IPv6 地址，则此规则合规。如果子网自动分配公共地址或地址，则此规则不合规。 IPv4 IPv6

> **Warning**
>
> 此规则不区分私有和公共全球单播地址 (GUA) IPv6 范围，并且在启用自动分配时会将所有 GUA 范围视为违规行为。

标识符：SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

资源类型： AWS::EC2::Subnet

触发器类型： 配置更改

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 Amazon Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResourceEvaluationAPI 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

有关主动评估的更多信息，请参阅评估模式。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

transfer-connector-logging-enabled

检查 Transf Amazon er Family Connector 是否向亚马逊发布日志 CloudWatch。如果没有为连接器分配，则该规则为 “不兼容”。 LoggingRole

标识符：TRANSFER_CONNECTOR_LOGGING_ENABLED

资源类型： AWS::Transfer::Connector

触发器类型： 配置更改

Amazon Web Services 区域：除中东（巴林）、亚太 Amazon 地区（泰国）、亚太地区（海得拉巴）、亚太地区（海得拉巴）、亚太地区（马来西亚）、亚太地区（墨尔本）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

vpc-endpoint-enabled

检查参数中指定的每项服务是否都具有 Amazon VPC 端点。如果 Amazon VPC 没有为每个指定服务创建 VPC 端点，则此规则为 NON_COMPLIANT。或者，您可以 VPCs 为要检查的规则指定某些内容。

标识符：VPC_ENDPOINT_ENABLED

资源类型： AWS::EC2::VPC

触发器类型： 定期

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（大阪）、亚太地区（马来西亚）、墨西哥（中部）、以色列（特拉维夫）、亚太地区（台北）、加拿大西部（卡尔加里）以外的所有支持区域

参数：

serviceNames, 类型：CSV

以逗号分隔的服务名称或端点列表。示例：“access-analyzer, appconfig, cloudtrail”或“com.amazonaws.region.access-analyzer”。 DescribeVpcEndpointServices 用于显示可用名称。

vpcIds（可选）, 类型：CSV

用逗号分隔的 VPC 终端节点的 Amazon V IDs PC 列表。如果提供，并且 serviceName 参数中指定的服务没有这些 VPC 端点之一，则该规则为 NON_COMPLIANT。

scopeConfigResource类型（可选）, 类型：CSV

以逗号分隔的 Con Amazon fig 资源类型列表，供规则检查。如果指定，则仅当账户中至少记录了一个指定资源时，该规则才会返回合规状态。例如：“AWS::SNS::Topic”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

vpc-flow-logs-enabled

检查是否为所有亚马逊找到并启用了亚马逊虚拟私有云（Amazon VPC）流日志 VPCs。如果没有为至少一个 Amazon VPC 启用流日志，则此规则为 NON_COMPLIANT。

标识符：VPC_FLOW_LOGS_ENABLED

资源类型： AWS::EC2::VPC

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

trafficType（可选），类型：字符串

TrafficType 的流日志

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

vpc-sg-open-only-to-authorized-ports

检查允许无限制传入流量的安全组（“0.0.0.0/0”或“::/0”）是否只允许授权端口上的传入 TCP 或 UDP 连接。如果此类安全组的规则参数中未指定端口，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则评估入口规则设置为 IPv4 ='0.0.0.0/0' 或 ='':: /' 的亚马逊 EC2 安全组。 IPv6如果安全组没有这些目的地之一，则此规则返回。NOT_APPLICABLE

标识符：VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

资源类型： AWS::EC2::SecurityGroup

触发器类型：配置更改和定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

authorizedTcpPorts （可选）, 类型：字符串

允许向 0.0.0.0/0 或 ::/0 开放的 TCP 端口的逗号分隔列表。以短划线定义范围，例如：“443,1020-1025”。

authorizedUdpPorts （可选）, 类型：字符串

允许向 0.0.0.0/0 或 ::/0 开放的 UDP 端口的逗号分隔列表。以短划线定义范围，例如：“500,1020-1025”。

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

wafv2-logging-enabled

检查是否在 Amazon WAFv2 区域和全球 Web 访问控制列表 (Web ACLs) 上启用了日志记录。如果启用了日志记录但日志记录目标与参数值不匹配，则此规则为 NON_COMPLIANT。

> **Note**
>
> Amazon Security Lake 异常
> 此规则不检查使用 Amazon WAFV2 网络版 Security Lake 完成的日志记录 ACLs。

标识符： WAFV2_LOGGIN G_已启用

资源类型： AWS::WAFv2::WebACL

触发器类型： 定期

Amazon Web Services 区域: 所有支持的 Amazon 区域

参数：

KinesisFirehoseDeliveryStreamArns （可选），类型：CSV

以逗号分隔的 Kinesis Firehose 直播列表 ARNs

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

wafv2-rulegroup-logging-enabled

检查是否启用了 Amazon WAFv2 规则组上的 Amazon CloudWatch 安全指标收集。如果是 '，则该规则不合规。VisibilityConfig CloudWatchMetricsEnabled'字段设置为假。

上下文： Amazon WAFV2 （Web 应用程序防火墙版本 2）允许您创建 Amazon WAF 规则来保护 Web 应用程序免受常见 Web 漏洞和漏洞的侵害。 Amazon WAF 规则组是一组可以与 Web ACL（访问控制列表）关联的 Amazon WAF 规则，用于定义 Web 应用程序流量所需的行为。有关更多信息，请参阅《Amazon WAF 开发人员指南》中的 Amazon WAF 规则和规则组。

通过在 Amazon WAFV2 规则组上配置 CloudWatch 安全指标收集，您可以监控安全指标，例如成功或失败的分布式拒绝服务 (DDoS)、SQL 注入和跨站点脚本 (XSS) 攻击。收集的安全指标可以帮助您简化调查。

> **Note**
>
> 如果 Amazon WAF 规则组中没有可供 Amazon Config 托管 Amazon WAFV2 规则检查的规则，则 Amazon Config 托管规则将返回`NOT_APPLICABLE`。

标识符： WAFV2_RULEGROUP_LOGIN G_ENABLED

资源类型： AWS::WAFv2::RuleGroup

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

wafv2-webacl-not-empty

检查 WAFv2 Web ACL 是否包含任何 WAF 规则或 WAF 规则组。如果 Web ACL 不包含任何 WAF 规则或 WAF 规则组，则此规则为 NON_COMPLIANT。

标识符： WAFV2_WEBACL_NOT_EMPTY

资源类型： AWS::WAFv2::WebACL

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（雅加达）、中东（阿联酋）、亚太地区（海得拉巴）、亚太地区（马来西亚）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）、欧洲（西班牙）、欧洲（苏黎世）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

waf-regional-rule-not-空

检查 WAF 区域规则是否包含条件。如果区域规则至少包含一个条件，则此规则为 COMPLIANT，否则为 NON_COMPLIANT。

标识符：WAF_REGIONAL_RULE_NOT_EMPTY

资源类型： AWS::WAFRegional::Rule

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

waf-regional-webacl-not-空

检查 WAF 区域 Web ACL 是否包含任何 WAF 规则或规则组。如果 Web ACL 中不存在任何 WAF 规则或规则组，则此规则为 NON_COMPLIANT。

标识符：WAF_REGIONAL_WEBACL_NOT_EMPTY

资源类型： AWS::WAFRegional::WebACL

触发器类型： 配置更改

Amazon Web Services 区域：除亚太 Amazon 地区（泰国）、亚太地区（马来西亚）、（美国东部）、（美国东部）Amazon GovCloud 、（美国西部）Amazon GovCloud 、墨西哥（中部）、亚太地区（台北）、加拿大西部（卡尔加里）地区以外的所有支持区域

参数：

无

Amazon CloudFormation 模板

要使用 Amazon CloudFormation 模板创建 Amazon Config 托管规则，请参阅使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则。

按评估模式列出的 Amazon Config 托管规则列表

Amazon Config 目前支持以下托管规则。在使用这些规则之前，请参阅 注意事项

主动评估

主动规则 是支持对尚未部署的资源采用主动评估模式的规则。这使您可以评估一组资源属性（如果用于定义 Amazon 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。有关更多信息，请参阅评估模式。

> **Note**
>
> 主动规则不会修复标记为 NON_COMPLIANT 的资源，也不会阻止部署这些资源。

主动评估

- eip-attached

侦查评估

侦查规则 是支持已部署资源的侦查评估模式的规则。这允许您评估现有资源的配置设置。

> **Note**
>
> 目前，所有 Amazon Config 规则都支持侦探评估。

侦查评估

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description

- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-在休息时
- appsync-cache-ct-encryption在途中
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标

- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-限制
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-已配置
- cloudfront-distribution-key-group-已启用
- cloudfront-no-deprecated-ssl-协议
- cloudfront-origin-access-identity-已启用
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-oac已启用
- 云前-3-origin-access-control-enabled
- 云前-3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-已加密
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check

- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用

- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-记录
- dms-replication-task-tagged
- dms-replication-task-targetdb-记录
- docdb-cluster-audit-logging-已启用

- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划

- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密

- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted

- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-启用身份验证
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查

- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-saml-provider-tagged
- iam-server-certificate-expiration-检查
- iam-server-certificate-tagged
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-no-policies-检查
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged

- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查

- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-需要-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用

- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption

- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用

- root-account-mfa-enabled
- 53 号公路-health-check-tagged
- 53 号公路-hosted-zone-tagged
- 53 号公路-query-logging-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-default-security-group-已关闭
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-空
- waf-global-rule-not-空
- waf-global-webacl-not-空
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

按触发器类型列出的 Amazon Config 托管规则列表

Amazon Config 目前支持以下托管规则。在使用这些规则之前，请参阅 注意事项

配置更改

变更触发的规则是 Amazon Config 根据配置更改进行评估的规则。

配置更改

- acmpca-certificate-authority-tagged
- acm-certificate-rsa-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-已启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密

- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicate到 ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged

- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-authorization-check
- appsync-cache-ct-encryption-在休息时
- appsync-cache-ct-encryption在途中
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled

- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-限制
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-已配置
- cloudfront-distribution-key-group-已启用
- cloudfront-no-deprecated-ssl-协议
- cloudfront-origin-access-identity-已启用
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-oac已启用
- 云前线-3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-已加密
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-settings-check
- cloudwatch-metric-stream-tagged
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-网址检查
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用

- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured

- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-task-sourcedb-记录
- dms-replication-task-tagged
- dms-replication-task-targetdb-记录
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-禁止
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ebs-snapshot-block-public-访问
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记

- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root 目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- eip-attached

- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-supported-version
- eks-fargate-profile-tagged
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl 检查
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl 检查
- elb-tagged
- elb-tls-https-listeners-只有
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description

- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- iam-customer-policy-blocked-kms 动作
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-oidc-provider-tagged
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-saml-provider-tagged
- iam-server-certificate-tagged

- iam-user-group-membership-检查
- iam-user-no-policies-检查
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记

- ivs-recording-configuration-tagged
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-需要-tls

- msk-unrestricted-access-check
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-tagged
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查

- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- required-tags
- 53 号公路-health-check-tagged
- 53 号公路-hosted-zone-tagged
- 53 号公路-query-logging-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-访问检查
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-using-cmk
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- ses-sending-tls-required

- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-default-security-group-已关闭
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-空
- waf-global-rule-not-空
- waf-global-webacl-not-空
- waf-regional-rulegroup-not-空

- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

定期

定期规则是按照您指定的频率定期 Amazon Config 评估的规则，例如，每 24 小时评估一次。

定期

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-已禁用
- alb-http-to-https-重定向检查
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-休息
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- 云前线-3-origin-non-existent-bucket
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- dms-replication-not-public
- docdb-cluster-encrypted-in-交通
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-resources-protected-by-备份计划
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-public-restorable-检查
- ec2-client-vpn-not-authorize-全部
- ec2-ebs-encryption-by-default
- ec2-已last-backup-recovery-point创建
- ec2-meets-restore-time-target
- ec2-resources-in-logically-air-gapped-vault

- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ecr-private-image-scanning-已启用
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eks-cluster-logging-enabled
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- event-data-store-cmk-已启用加密
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-已启用
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-检查
- iam-server-certificate-expiration-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- inspector-ec2-scan-enabled

- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- kinesis-firehose-delivery-stream-已加密
- kms-cmk-not-scheduled-用于删除
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-automatic-minor-version-已启用升级
- mq-cloudwatch-audit-logging-已启用
- mq-no-public-access
- multi-region-cloud-trail-已启用
- netfw-logging-enabled
- nlb-logging-enabled
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-mysql-instance-encrypted在途中
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-sqlserver-encrypted-in-交通
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中

- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- s3--account-level-public-access 区块-周期性
- s3-已last-backup-recovery-point创建
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- transfer-family-server-no-ftp

- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-port-restriction-检查
- wafv2-logging-enabled
- waf-classic-logging-enabled

Hybrid

混合规则是针对配置更改 Amazon Config 进行评估和定期评估的规则。

Hybrid

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-检查
- ec2-instance-launched-with-allowed-ami
- incoming-ssh-disabled
- no-unrestricted-route-to-igw
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

按区域可用性列出的 Amazon Config 托管规则列表

Amazon Config 目前支持以下托管规则。在使用这些规则之前，请参阅 注意事项

美国东部（俄亥俄州）区域

美国东部（俄亥俄州）

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-启用标头
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用

- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标

- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az

- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用

- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- 代码部署-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured

- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault

- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled

- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az

- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- frauddetector-entity-type-tagged
- frauddetector-label-tagged

- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作

- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证

- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-需要-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包

- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用

- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块

- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置

- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-default-security-group-已关闭
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

美国东部（弗吉尼亚州北部）区域

美国东部（弗吉尼亚州北部）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-启用标头
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged

- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description

- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-在休息时
- appsync-cache-ct-encryption在途中
- appsync-cache-encryption-at-休息

- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查

- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-已配置
- cloudfront-distribution-key-group-已启用
- cloudfront-no-deprecated-ssl-协议
- cloudfront-origin-access-identity-已启用
- cloudfront-origin-failover-enabled
- cloudfront-origin-lambda-url-oac已启用
- 云前线-3-origin-access-control-enabled
- 云前线-3-origin-non-existent-bucket
- cloudfront-security-policy-check

- cloudfront-sni-enabled
- cloudfront-ssl-policy-check
- cloudfront-traffic-to-origin-已加密
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用

- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- 代码部署-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-记录
- dms-replication-task-tagged
- dms-replication-task-targetdb-记录
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required

- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged

- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分

- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在

- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-oidc-provider-tagged
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-saml-provider-tagged
- iam-server-certificate-expiration-检查
- iam-server-certificate-tagged
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-no-policies-检查
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用

- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-已加密

- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-需要-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged

- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查

- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check

- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- 53 号公路-health-check-tagged
- 53 号公路-hosted-zone-tagged
- 53 号公路-query-logging-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited

- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-default-security-group-已关闭
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-空
- waf-global-rule-not-空
- waf-global-webacl-not-空
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

美国西部（北加利福尼亚）区域

美国西部（北加利福尼亚）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-启用标头
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged

- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged

- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description

- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- 代码部署-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged

- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance

- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged

- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached

- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit

- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划

- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查

- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-检查
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级

- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged

- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查

- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

美国西部（俄勒冈州）区域

美国西部（俄勒冈州）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-启用标头
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用

- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查

- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用

- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled

- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志

- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- 代码部署-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled

- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted

- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-spot-fleet-request-ct-encryption-at-rest

- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制

- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled

- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access

- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查

- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查

- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description

- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限

- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用

- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查

- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问

- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-default-security-group-已关闭
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports

- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

非洲（开普敦）区域

非洲（开普敦）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-启用标头
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled

- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description

- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标

- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新

- 代码部署-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志

- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description

- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged

- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作

- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted

- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable

- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted

- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划

- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用

- workspaces-workspace-tagged

亚太地区（香港）区域

亚太地区（香港）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured

- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on

- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限

- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查

- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-记录
- dms-replication-task-tagged
- dms-replication-task-targetdb-记录
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted

- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled

- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description

- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查

- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时

- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息

- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled

- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp

- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分

- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl

- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-no-公共访问
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

亚太地区（海得拉巴）区域

亚太地区（海得拉巴）

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查

- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级

- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-限制
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check

- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查

- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标

- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-stopped-instance

- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本

- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-已启用
- iam-password-policy
- iam-root-access-key-检查
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc

- lambda-vpc-multi-az-检查
- mariadb-publish-logs-to-云监视日志
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-启用日志功能
- rds-automatic-minor-version-已启用升级
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged

- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记

- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-访问
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled

- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

亚太地区（雅加达）区域

亚太地区（雅加达）

- access-keys-rotated
- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm

- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置

- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- clb-desync-mode-check

- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https

- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问

- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本

- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用

- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查

- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-no-公共访问
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-no-public-访问
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description

- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

亚太地区（马来西亚）区域

亚太地区（马来西亚）

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-重定向检查
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf

- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launch-config-public-ip 已禁用
- beanstalk-enhanced-health-reporting-已启用
- cloudformation-stack-drift-detection-检查
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- cw-loggroup-retention-period-检查
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-访问

- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-备份检查
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-已启用
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kms-cmk-not-scheduled-用于删除
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- multi-region-cloud-trail-已启用
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled

- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3--account-level-public-access 区块-周期性
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip 已禁用
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

亚太地区（墨尔本）区域

亚太地区（墨尔本）

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description

- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- approved-amis-by-id
- approved-amis-by-tag
- appsync-graphql-api-xray-已启用
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description

- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查

- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami

- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用

- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged

- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-redis-cluster-automatic-备份检查
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fms-shield-resource-policy-检查

- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-deployment-type-检查
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-已启用
- iam-password-policy
- iam-root-access-key-检查
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-只有

- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- mariadb-publish-logs-to-云监视日志
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-log-已启用
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-启用日志功能
- rds-automatic-minor-version-已启用升级
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support

- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- 53 号公路-resolver-resolver-rule-tagged

- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-config-prod-实例计数

- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-访问
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled

- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

亚太地区（孟买）区域

亚太地区（孟买）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description

- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged

- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check

- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用

- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-记录
- dms-replication-task-tagged
- dms-replication-task-targetdb-记录
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description

- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份

- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version

- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在

- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled

- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged

- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查

- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用

- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version

- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled

- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建

- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled

- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

亚太地区（大阪）区域

亚太地区（大阪）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查

- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged

- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-envvar-awscred-检查

- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged

- dms-mongo-db-authentication-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-tagged
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged

- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description

- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查

- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- macie-auto-sensitive-data-发现-检查
- macie-status-check

- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled

- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息

- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled

- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault

- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

亚太地区（首尔）区域

亚太地区（首尔）

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-已启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用

- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check

- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项

- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check

- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check

- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public

- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用

- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair

- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled

- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled

- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled

- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查

- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access

- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled

- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan

- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用

- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本

- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description

- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

亚太地区（新加坡）区域

亚太地区（新加坡）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-已启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed

- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls

- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置

- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged

- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查

- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https

- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled

- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密

- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件

- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description

- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description

- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用

- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc

- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check

- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中

- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用

- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused

- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp

- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

亚太地区（悉尼）区域

亚太地区（悉尼）

- access-keys-rotated
- account-part-of-organizations

- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-已启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记

- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check

- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分

- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged

- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check

- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged

- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分

- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在

- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- frauddetector-entity-type-tagged
- frauddetector-label-tagged
- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged

- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description

- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用

- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中

- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问

- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only

- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

亚太地区（台北）区域

亚太地区（台北）

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-重定向检查

- approved-amis-by-id
- approved-amis-by-tag
- cloudformation-stack-drift-detection-检查
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- cw-loggroup-retention-period-检查
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-检查
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check

- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- multi-region-cloud-trail-已启用
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3--account-level-public-access 区块-周期性

- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- subnet-auto-assign-public-ip 已禁用
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

亚太地区（泰国）区域

亚太地区（泰国）

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-重定向检查
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed

- api-gw-execution-logging-已启用
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- cloudformation-stack-drift-detection-检查
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- cw-loggroup-retention-period-检查
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-检查
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami

- ec2-instance-managed-by-ssm
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-备份检查
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-已启用
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc

- kms-cmk-not-scheduled-用于删除
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- multi-region-cloud-trail-已启用
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3--account-level-public-access 区块-周期性
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-level-public-access-禁止使用
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip 已禁用
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

亚太地区（东京）区域

亚太地区（东京）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled

- amplify-app-branch-auto-已启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description

- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged

- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check

- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志

- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged

- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check

- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本

- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问

- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check

- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置

- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查

- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description

- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限

- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用

- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查

- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc

- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查

- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up

- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

加拿大（中部）区域

加拿大（中部）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-已启用删除

- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description

- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-限制
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled

- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证

- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-已启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上

- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled

- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建

- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-分析已network-insights-access-scope标记
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-已禁用附件

- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description

- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查

- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作

- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iot-authorizer-token-signing-已启用

- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode

- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包

- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled

- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged

- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged

- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty

- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

Canada West（Calgary）Region

加拿大西部（卡尔加里）

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged

- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- approved-amis-by-id
- approved-amis-by-tag
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- aurora-mysql-cluster-audit-记录
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launch-config-public-ip 已禁用
- batch-scheduling-policy-tagged
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check

- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- cw-loggroup-retention-period-检查
- datasync-task-data-verification-已启用
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-prefix-list-tagged
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-tagged
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-encrypted-check
- efs-file-system-tagged
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-备份检查
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- glb-tagged
- glue-ml-transform-tagged
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kms-cmk-not-scheduled-用于删除
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- mariadb-publish-logs-to-云监视日志
- multi-region-cloud-trail-已启用
- netfw-subnet-change-protection-已启用
- nlb-internal-scheme-check
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-已启用升级
- rds-cluster-deletion-protection-已启用
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3--account-level-public-access 区块-周期性
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- subnet-auto-assign-public-ip 已禁用
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

中国（北京）区域

中国（北京）

- access-keys-rotated
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-重定向检查

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-execution-logging-已启用
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-休息
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-记录
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- 云前线-3-origin-non-existent-bucket
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-environment-privileged-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-report-group-encrypted-在休息时
- cognito-identity-pool-unauth-访问检查
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-task-logging-enabled
- dax-encryption-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-记录
- dms-replication-task-targetdb-记录
- docdb-cluster-encrypted-in-交通
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-deletion-protection-已启用
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-访问

- ebs-snapshot-public-restorable-检查
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root 目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-auto-minor-version-升级检查
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check

- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-ontap-deployment-type-检查
- fsx-openzfs-deployment-type-检查
- fsx-windows-deployment-type-检查
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-spark-job-supported-版本
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms 动作
- iam-inline-policy-blocked-kms 动作
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- lambda-function-public-access-禁止

- lambda-function-xray-enabled
- lambda-vpc-multi-az-检查
- mfa-enabled-for-iam-控制台访问权限
- mq-active-deployment-mode
- mq-auto-minor-version-已启用升级
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-subnet-change-protection-已启用
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-update-check
- rabbit-mq-supported-version
- rds-enhanced-monitoring-enabled
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-instance-encrypted在途中
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用

- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-routes-在 vpc 内
- required-tags
- restricted-incoming-traffic
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-密钥已配置

- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-启用日志功能
- subnet-auto-assign-public-ip 已禁用
- transfer-connector-logging-enabled
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-空

- waf-regional-webacl-not-空

中国（宁夏）区域

中国（宁夏）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-重定向检查
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-execution-logging-已启用
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-休息
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-日志
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查

- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-environment-privileged-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-report-group-encrypted-在休息时
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-task-logging-enabled
- dax-encryption-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-replication-instance-multi-az 已启用

- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-table-deletion-protection-已启用
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest

- ec2-stopped-instance
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-auto-minor-version-升级检查
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时

- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-ontap-deployment-type-检查
- fsx-openzfs-deployment-type-检查
- fsx-windows-deployment-type-检查
- glue-job-logging-enabled
- glue-spark-job-supported-版本
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms 动作
- iam-inline-policy-blocked-kms 动作
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access

- iam-root-access-key-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- mfa-enabled-for-iam-控制台访问权限
- mq-active-deployment-mode
- mq-auto-minor-version-已启用升级
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- netfw-subnet-change-protection-已启用
- no-unrestricted-route-to-igw
- opensearch-update-check

- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-休息
- rds-enhanced-monitoring-enabled
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-logging-enabled
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-routes-在 vpc 内
- required-tags

- restricted-incoming-traffic
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- step-functions-state-machine-启用日志功能
- subnet-auto-assign-public-ip 已禁用
- transfer-connector-logging-enabled
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用

欧洲地区（法兰克福）区域

欧洲地区（法兰克福）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled

- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-在休息时
- appsync-cache-ct-encryption在途中
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时

- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时

- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled

- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2 network-insights-access-scope-分析标签
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root 目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan

- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged

- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled

- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged

- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged
- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check

- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required

- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中

- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问

- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only

- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-default-security-group-已关闭
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

欧洲地区（爱尔兰）区域

欧洲地区（爱尔兰）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled

- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志

- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check

- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新

- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用

- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问

- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2 network-insights-access-scope-分析标签

- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled

- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root 目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az

- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- frauddetector-entity-type-tagged
- frauddetector-label-tagged

- frauddetector-outcome-tagged
- frauddetector-variable-tagged
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作

- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iotsitewise-asset-model-tagged
- iotsitewise-dashboard-tagged
- iotsitewise-gateway-tagged
- iotsitewise-portal-tagged
- iotsitewise-project-tagged

- iottwinmaker-component-type-tagged
- iottwinmaker-entity-tagged
- iottwinmaker-scene-tagged
- iottwinmaker-sync-job-tagged
- iottwinmaker-workspace-tagged
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- ivs-channel-playback-authorization-已启用
- ivs-channel-tagged
- ivs-playback-key-pair-已标记
- ivs-recording-configuration-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check

- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查

- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查

- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check

- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled

- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged

- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-default-security-group-已关闭
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

欧洲地区（伦敦）区域

欧洲地区（伦敦）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged

- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled

- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appintegrations-event-integration-description
- appintegrations-event-integration-tagged
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists

- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问
- apprunner-service-observability-enabled
- apprunner-service-tagged
- appstream-fleet-in-vpc
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- auditmanager-assessment-tagged
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled

- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查

- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚

- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- connect-instance-logging-enabled
- customerprofiles-domain-tagged
- customerprofiles-object-type-allow-创建个人资料
- customerprofiles-object-type-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分

- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2 network-insights-access-scope-分析标签
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用

- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root 目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault

- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用

- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用

- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iotevents-alarm-model-tagged
- iotevents-detector-model-tagged
- iotevents-input-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问

- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标

- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密

- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled

- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

欧洲地区（米兰）

欧洲地区（米兰）

- access-keys-rotated

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用

- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged

- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted

- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached

- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划

- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check

- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2 network-insights-access-scope-分析标签
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用

- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root 目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标

- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查

- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查

- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use

- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限

- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分

- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-unrestricted-port-access

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged

- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

欧洲地区（巴黎）区域

欧洲地区（巴黎）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查

- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description

- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- apprunner-service-in-vpc
- apprunner-service-ip-address-类型检查
- apprunner-service-max-unhealthy-阈值
- apprunner-service-no-public-访问

- apprunner-service-observability-enabled
- apprunner-service-tagged
- apprunner-vpc-connector-tagged
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-backtracking-enabled
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护

- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-记录
- dms-replication-task-tagged
- dms-replication-task-targetdb-记录
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted

- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-carrier-gateway-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check

- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2 network-insights-access-scope-分析标签
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户

- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移

- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip

- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description

- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级

- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空

- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查

- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记

- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited

- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged

- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能

- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空

- waf-regional-webacl-not-空

欧洲（西班牙）区域

欧洲（西班牙）

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time

- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用

- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用

- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划

- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check

- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查

- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only

- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-managed-updates-已启用
- elbv2-multiple-az
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查

- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-已启用
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged

- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- mariadb-publish-logs-to-云监视日志
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-启用日志功能
- rds-automatic-minor-version-已启用升级
- rds-cluster-default-admin-检查

- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3--account-level-public-access 区块-周期性

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-密钥已配置

- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-访问
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description

- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

欧洲地区（斯德哥尔摩）区域

欧洲地区（斯德哥尔摩）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除

- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged

- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置

- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged

- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密

- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codeguruprofiler-profiling-group-tagged
- codegurureviewer-repository-association-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查

- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2 network-insights-access-scope-分析标签
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged

- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted

- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- evidently-launch-description
- evidently-launch-tagged
- evidently-project-description
- evidently-project-tagged
- evidently-segment-description
- evidently-segment-tagged
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查

- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access

- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-code-scan-已启用
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止

- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- lightsail-bucket-allow-public-重写-已禁用
- lightsail-bucket-tagged
- lightsail-certificate-tagged
- lightsail-disk-tagged
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp

- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch

- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check

- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic

- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- s3 express-dir-bucket-lifecycle-规则检查
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged

- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分

- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

欧洲（苏黎世）

欧洲（苏黎世）

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-tagged

- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时

- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-限制
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging

- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https

- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-spot-fleet-request-ct-encryption-at-rest
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件

- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-已启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan

- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elbv2-multiple-az
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-已启用加密
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用

- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-已启用
- iam-password-policy
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- mariadb-publish-logs-to-云监视日志

- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查

- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区

- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-encrypted在途中
- redshift-serverless-workgroup-no-公共访问
- redshift-serverless-workgroup-routes-在 vpc 内
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-访问
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

以色列（特拉维夫）区域

以色列（特拉维夫）

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空

- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-graphql-api-xray-已启用
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-配置

- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-mysql-cluster-audit-记录
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-限制
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- batch-scheduling-policy-tagged
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-envvar-awscred-检查

- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled

- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-prefix-list-tagged
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled

- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-file-system-tagged
- efs-in-backup-plan
- efs-mount-target-public-可访问
- eip-attached
- eks-cluster-secrets-encrypted
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-redis-cluster-automatic-备份检查
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elbv2-multiple-az
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-启用加密
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-lustre-copy-tags到备份
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-windows-deployment-type-检查
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时

- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- kinesis-firehose-delivery-stream-已加密
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- macie-auto-sensitive-data-发现-检查
- mariadb-publish-logs-to-云监视日志

- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-启用日志功能
- rds-automatic-minor-version-已启用升级
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged

- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查

- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-no-公共访问
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check

- sagemaker-app-image-config-已标记
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-no-public-访问
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- subnet-auto-assign-public-ip 已禁用
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp

- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

墨西哥（中部）区域

墨西哥（中部）

- account-part-of-organizations
- acm-certificate-expiration-check
- alb-http-to-https-重定向检查
- apigatewayv2-stage-description
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-execution-logging-已启用
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- cloudformation-stack-drift-detection-检查
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check

- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- cw-loggroup-retention-period-检查
- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-snapshot-public-restorable-检查
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check

- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-备份检查
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kms-cmk-not-scheduled-用于删除
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- multi-region-cloud-trail-已启用
- no-unrestricted-route-to-igw
- rds-enhanced-monitoring-enabled
- rds-in-backup-plan
- rds-logging-enabled
- required-tags
- restricted-incoming-traffic
- s3--account-level-public-access 区块-周期性
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip 已禁用
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

中东（巴林）区域

中东（巴林）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version

- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged

- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-在休息时

- appsync-cache-ct-encryption在途中
- appsync-cache-encryption-at-休息
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled

- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-记录
- dms-replication-task-tagged
- dms-replication-task-targetdb-记录
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划

- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2 network-insights-access-scope-分析标签
- ec2-已network-insights-access-scope标记

- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access

- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version

- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description
- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check

- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-openzfs-copy-tags-已启用
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- glb-listener-tagged
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled

- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp

- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用

- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled

- opensearch-audit-logging-enabled
- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-meets-restore-time-目标
- rds-multi-az-support

- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list

- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target

- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知

- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-default-security-group-已关闭
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查

- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

中东（阿联酋）区域

中东（阿联酋）：

- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check
- alb-tagged
- alb-waf-enabled
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密

- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time
- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-extension-association-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-记录
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed
- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- clb-multiple-az
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https
- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-replication-not-public
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default

- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-stopped-instance
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-transit-gateway-auto-vpc-禁用附件
- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置

- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-根目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached

- eks-addon-tagged
- eks-cluster-log-enabled
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-redis-cluster-automatic-备份检查
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-managed-updates-已启用
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes

- event-data-store-cmk-启用加密
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-tagged
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-external-access-analyzer-已启用

- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotdevicedefender-custom-metric-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- iot-scheduled-audit-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- mariadb-publish-logs-to-云监视日志
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-auto-minor-version-已启用升级

- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-internal-scheme-check
- nlb-logging-enabled
- nlb-tagged

- no-unrestricted-route-to-igw
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption

- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-no-公共访问
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-

- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-image-description

- sagemaker-image-tagged
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-no-public-访问
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged

- transfer-connector-logging-enabled
- transfer-connector-tagged
- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- waf-regional-rule-not-空
- waf-regional-webacl-not-空

南美洲（圣保罗）区域

南美洲（圣保罗）

- access-keys-rotated
- account-part-of-organizations
- acmpca-certificate-authority-tagged
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-已禁用
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-drop-invalid-已启用标题
- alb-http-to-https-重定向检查
- alb-internal-scheme-check

- alb-listener-tagged
- alb-tagged
- alb-waf-enabled
- amplify-app-branch-auto-已启用删除
- amplify-app-description
- amplify-app-no-environment-变量
- amplify-app-tagged
- amplify-branch-description
- amplify-branch-performance-mode-已启用
- amplify-branch-tagged
- apigatewayv2-stage-description
- apigateway-stage-access-logs-已启用
- apigateway-stage-description
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gwv2--启用指标 stage-default-route-detailed
- api-gw-associated-with-waf
- api-gw-cache-enabled并已加密
- api-gw-endpoint-type-检查
- api-gw-execution-logging-已启用
- api-gw-rest-api-已标记
- api-gw-ssl-enabled
- api-gw-stage-tagged
- api-gw-xray-enabled
- appconfig-application-description
- appconfig-application-tagged
- appconfig-configuration-profile-tagged
- appconfig-configuration-profile-validators-不为空
- appconfig-deployment-strategy-description
- appconfig-deployment-strategy-minimum-final-bake-time

- appconfig-deployment-strategy-replicateto-ssm
- appconfig-deployment-strategy-tagged
- appconfig-environment-description
- appconfig-environment-tagged
- appconfig-extension-association-tagged
- appconfig-freeform-profile-config-存储
- appconfig-hosted-configuration-version-描述
- appflow-flow-tagged
- appflow-flow-trigger-type-检查
- appmesh-gateway-route-tagged
- appmesh-mesh-deny-tcp-转发
- appmesh-mesh-tagged
- appmesh-route-tagged
- appmesh-virtual-gateway-backend-默认值-tls
- appmesh-virtual-gateway-logging-file-path-exists
- appmesh-virtual-gateway-tagged
- appmesh-virtual-node-backend-defaults-tls-on
- appmesh-virtual-node-cloud-map-ip-pref-check
- appmesh-virtual-node-dns-ip-pref-check
- appmesh-virtual-node-logging-file-path-exists
- appmesh-virtual-node-tagged
- appmesh-virtual-router-tagged
- appmesh-virtual-service-tagged
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-ct-encryption-在休息时
- appsync-cache-ct-encryption在途中
- appsync-cache-encryption-at-休息

- appsync-graphql-api-xray-已启用
- appsync-logging-enabled
- aps-rule-groups-namespace-已标记
- athena-data-catalog-description
- athena-prepared-statement-description
- athena-workgroup-description
- athena-workgroup-encrypted-at-休息
- athena-workgroup-enforce-workgroup-配置
- athena-workgroup-engine-version-自动升级
- athena-workgroup-logging-enabled
- aurora-global-database-encryption-在休息时
- aurora-last-backup-recovery-已创建积分
- aurora-meets-restore-time-目标
- aurora-mysql-cluster-audit-日志
- aurora-resources-in-logically-air-gapped-vault
- aurora-resources-protected-by-备份计划
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-必填项
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-极限
- autoscaling-launch-config-public-ip 已禁用
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-已禁用
- backup-recovery-point-minimum-保留检查
- batch-compute-environment-enabled
- batch-compute-environment-managed

- batch-compute-environment-tagged
- batch-job-queue-enabled
- batch-job-queue-tagged
- batch-managed-compute-environment-using-launch-template
- batch-managed-compute-env-allocation-strategy-check
- batch-managed-compute-env-compute-resources-tagged
- batch-managed-spot-compute-environment-max-bid
- batch-scheduling-policy-tagged
- beanstalk-enhanced-health-reporting-已启用
- cassandra-keyspace-tagged
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-notification-check
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-检查
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloudwatch-metric-stream-tagged
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-检查
- codebuild-project-envvar-awscred-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-project-source-repo-url-check
- codebuild-report-group-encrypted-在休息时
- codebuild-report-group-tagged
- codedeploy-auto-rollback-monitor-已启用
- codedeploy-deployment-group-auto-启用回滚
- codedeploy-deployment-group-outdated-实例更新
- codeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-禁用
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- cognito-identity-pool-unauthenticated-登录
- cognito-identity-pool-unauth-访问检查
- cognito-userpool-cust-auth-threat-full-check
- cognito-user-pool-advanced-已启用安全性
- cognito-user-pool-deletion-启用保护
- cognito-user-pool-mfa-已启用
- cognito-user-pool-password-政策检查
- cognito-user-pool-tagged
- custom-eventbus-policy-attached
- custom-schema-registry-policy-已附上
- cw-loggroup-retention-period-检查
- datasync-location-object-storage-使用-https

- datasync-task-data-verification-已启用
- datasync-task-logging-enabled
- datasync-task-tagged
- dax-encryption-enabled
- dax-tls-endpoint-encryption
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-升级检查
- dms-endpoint-ssl-configured
- dms-endpoint-tagged
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- dms-replication-task-sourcedb-日志
- dms-replication-task-tagged
- dms-replication-task-targetdb-日志
- docdb-cluster-audit-logging-已启用
- docdb-cluster-backup-retention-检查
- docdb-cluster-deletion-protection-已启用
- docdb-cluster-encrypted
- docdb-cluster-encrypted-in-交通
- docdb-cluster-snapshot-public-禁止
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-meets-restore-time-目标
- dynamodb-pitr-enabled

- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-meets-restore-time-目标
- ebs-optimized-instance
- ebs-resources-in-logically-air-gapped-vault
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-capacity-reservation-tagged
- ec2-已client-vpn-connection-log启用
- ec2-client-vpn-endpoint-tagged
- ec2-client-vpn-not-authorize-全部
- ec2-dhcp-options-tagged
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-fleet-tagged
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密

- ec launch-template-imdsv 2-2-check
- ec2-launch-template-public-ip-已禁用
- ec2-launch-template-tagged
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2 network-insights-access-scope-分析标签
- ec2-已network-insights-access-scope标记
- ec2-network-insights-analysis-tagged
- ec2-network-insights-path-tagged
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-prefix-list-tagged
- ec2-resources-in-logically-air-gapped-vault
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-peric
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-traffic-mirror-filter-description
- ec2-traffic-mirror-filter-tagged
- ec2-traffic-mirror-session-description
- ec2-traffic-mirror-session-tagged
- ec2-traffic-mirror-target-description
- ec2-traffic-mirror-target-tagged
- ec2-transit-gateway-auto-vpc-禁用附件

- ec2-已transit-gateway-multicast-domain标记
- ec2-volume-inuse-check
- ec2-vpn-connection-logging-enabled
- ec2-vpn-connection-tagged
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecr-repository-tagged
- ecs-awsvpc-networking-enabled
- ecs-capacity-provider-tagged
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-no-environment-secrets
- ecs-task-definition-efs-启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-log-配置
- ecs-task-definition-memory-硬限制
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-nonroot-用户
- ecs-task-definition-pid-模式检查
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-root 目录
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check

- efs-filesystem-ct-encrypted
- efs-file-system-tagged
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-meets-restore-time-目标
- efs-mount-target-public-可访问
- efs-resources-in-logically-air-gapped-vault
- efs-resources-protected-by-备份计划
- eip-attached
- eks-addon-tagged
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-版本
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-fargate-profile-tagged
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-auto-minor-version-升级检查
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-备份检查
- elasticache-repl-grp-auto-启用故障转移
- elasticache-repl-grp-encrypted-在休息时
- elasticache-repl-grp-encrypted在途中
- elasticache-repl-grp-redis-已启用 auth
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticbeanstalk-application-description
- elasticbeanstalk-application-version-description

- elasticbeanstalk-environment-description
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-加密检查
- elastic-beanstalk-logs-to-云观察
- elastic-beanstalk-managed-updates-已启用
- elbv2-acm-certificate-required
- elbv2-listener-encryption-in-transit
- elbv2-multiple-az
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-cross-zone-load-启用平衡
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-internal-scheme-check
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tagged
- elb-tls-https-listeners-只有
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- emr-security-configuration-encryption-休息
- emr-security-configuration-encryption-交通
- encrypted-volumes
- event-data-store-cmk-启用加密
- fis-experiment-template-log-配置-存在
- fis-experiment-template-tagged
- fms-shield-resource-policy-检查

- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-lustre-copy-tags到备份
- fsx-meets-restore-time-目标
- fsx-ontap-deployment-type-检查
- fsx-openzfs-copy-tags-已启用
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-audit-log-已配置
- fsx-windows-deployment-type-检查
- glb-listener-tagged
- glb-tagged
- global-endpoint-event-replication-已启用
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-ml-transform-tagged
- glue-spark-job-supported-版本
- guardduty-ec2-protection-runtime-enabled
- guardduty-ecs-protection-runtime-已启用
- guardduty-eks-protection-audit-已启用
- guardduty-eks-protection-runtime-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-malware-protection-enabled
- guardduty-non-archived-findings
- guardduty-rds-protection-enabled
- guardduty-runtime-monitoring-enabled
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作

- iam-external-access-analyzer-已启用
- iam-group-has-users-检查
- iam-inline-policy-blocked-kms 动作
- iam-no-inline-policy-检查
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-检查
- iam-root-access-key-检查
- iam-user-group-membership-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- internet-gateway-authorized-vpc-只有
- iotwireless-fuota-task-tagged
- iotwireless-multicast-group-tagged
- iotwireless-service-profile-tagged
- iot-authorizer-token-signing-已启用
- iot-job-template-tagged
- iot-provisioning-template-description
- iot-provisioning-template-jitp
- iot-provisioning-template-tagged
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查

- kinesis-stream-encrypted
- kinesis-video-stream-minimum-数据保留
- kms-cmk-not-scheduled-用于删除
- kms-key-policy-no-公共访问
- kms-key-tagged
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-description
- lambda-function-public-access-禁止
- lambda-function-settings-check
- lambda-function-xray-enabled
- lambda-inside-vpc
- lambda-vpc-multi-az-检查
- macie-auto-sensitive-data-发现-检查
- macie-status-check
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-active-broker-ldap-认证
- mq-active-deployment-mode
- mq-active-single-instance-broker-storage-type-efs
- mq-automatic-minor-version-已启用升级
- mq-auto-minor-version-已启用升级
- mq-broker-general-logging-已启用
- mq-cloudwatch-audit-logging-已启用
- mq-cloudwatch-audit-log-已启用
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-cluster-public-access-已禁用
- msk-cluster-tagged
- msk-connect-connector-logging-已启用

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-requi-tls
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-检查
- neptune-cluster-cloudwatch-log-启用导出
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-已启用
- neptune-cluster-encrypted
- neptune-cluster-iam-database-认证
- neptune-cluster-multi-az-已启用
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-禁止
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-碎片数据包
- netfw-policy-default-action-满包
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-cross-zone-load-启用平衡
- nlb-internal-scheme-check
- nlb-listener-tagged
- nlb-logging-enabled
- nlb-tagged
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-容忍
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-加密检查
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-mysql-audit-启用日志功能
- rds-aurora-postgresql-logs到云端观察
- rds-automatic-minor-version-已启用升级
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-检查
- rds-cluster-deletion-protection-已启用
- rds-cluster-encrypted-at-休息
- rds-cluster-iam-authentication-已启用
- rds-cluster-multi-az-已启用
- rds-db-security-group-不允许
- rds-enhanced-monitoring-enabled
- rds-event-subscription-tagged
- rds-instance-default-admin-检查
- rds-instance-deletion-protection-已启用
- rds-instance-iam-authentication-已启用
- rds-instance-public-access-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中

- rds-meets-restore-time-目标
- rds-multi-az-support
- rds-mysql-cluster-copy-tags-to-snapshot-check
- rds-mysql-instance-encrypted在途中
- rds-option-group-tagged
- rds-pgsql-cluster-copy-tags-to-snapshot-check
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-proxy-tls-encryption
- rds-resources-protected-by-备份计划
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-parameter-group-已标记
- redshift-cluster-public-access-检查
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-default-db-name-检查
- redshift-enhanced-vpc-routing-已启用
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查

- redshift-serverless-namespace-cmk-加密
- redshift-serverless-publish-logs到云端观察
- redshift-serverless-workgroup-no-公共访问
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-已启用
- root-account-mfa-enabled
- route53--已标记 resolver-firewall-domain-list
- route53-协会已标记 resolver-firewall-rule-group
- route53--已标记 resolver-firewall-rule-group
- 53 号公路-resolver-resolver-rule-tagged
- rum-app-monitor-cloudwatch-启用日志
- rum-app-monitor-tagged
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3 account-level-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-禁止使用
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-bucket-tagged
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-in-logically-air-gapped-vault
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-app-image-config-已标记
- sagemaker-domain-in-vpc
- sagemaker-domain-tagged
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-feature-group-tagged
- sagemaker-image-description
- sagemaker-image-tagged
- sagemaker-model-in-vpc
- sagemaker-model-isolation-enabled
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-instance-root-访问检查
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-检查
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- service-catalog-portfolio-tagged
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sns-encrypted-kms
- sns-topic-message-delivery-启用通知
- sns-topic-no-public-访问
- sqs-queue-dlq-check
- sqs-queue-no-public-访问
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- ssm-document-tagged
- stepfunctions-state-machine-tagged
- step-functions-state-machine-启用日志功能
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-in-logically-air-gapped-vault
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-agreement-description
- transfer-agreement-tagged
- transfer-certificate-description
- transfer-certificate-tagged
- transfer-connector-logging-enabled
- transfer-connector-tagged

- transfer-family-server-no-ftp
- transfer-profile-tagged
- transfer-workflow-description
- transfer-workflow-tagged
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-in-logically-air-gapped-vault
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-network-acl-unused-检查
- vpc-peering-dns-resolution-检查
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-空
- waf-regional-rule-not-空
- waf-regional-webacl-not-空
- workspaces-connection-alias-tagged
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用
- workspaces-workspace-tagged

Amazon GovCloud（美国东部）区域

Amazon GovCloud（美国东部）

- access-keys-rotated
- account-part-of-organizations

- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-重定向检查
- api-gw-execution-logging-已启用
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-已创建积分
- aurora-mysql-cluster-audit-记录
- aurora-resources-protected-by-备份计划
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-禁用
- backup-recovery-point-minimum-保留检查
- clb-desync-mode-check
- cloudformation-stack-drift-detection-检查
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check

- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-environment-privileged-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-report-group-encrypted-在休息时
- cw-loggroup-retention-period-检查
- datasync-task-logging-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled
- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- docdb-cluster-encrypted-in-交通
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问

- ebs-snapshot-public-restorable-检查
- ec2-已client-vpn-connection-log启用
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-task-definition-efs-启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host

- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-mount-target-public-可访问
- efs-resources-protected-by-备份计划
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-redis-cluster-automatic-备份检查
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-已启用
- elbv2-listener-encryption-in-transit
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-custom-security-policy-ssl-check
- elb-predefined-security-policy-ssl-check
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-启用加密
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查

- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-ontap-deployment-type-检查
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-deployment-type-检查
- glue-job-logging-enabled
- glue-spark-job-supported-版本
- guardduty-eks-protection-audit-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-inline-policy-blocked-kms 动作
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- lambda-function-public-access-禁止
- lambda-function-xray-enabled
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-cloudwatch-audit-log-已启用
- msk-cluster-public-access-已禁用
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-logging-enabled
- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs到云端观察
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-mysql-instance-encrypted在途中
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中

- rds-resources-protected-by-备份计划
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-unrestricted-port-access
- required-tags
- restricted-incoming-traffic
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3 resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- sqs-queue-dlq-check
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-protected-by-备份计划

- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

Amazon GovCloud（美国西部）区域

Amazon GovCloud（美国西部）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- active-mq-supported-version
- alb-desync-mode-check
- alb-http-to-https-重定向检查
- api-gw-execution-logging-已启用
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-logging-enabled
- aurora-last-backup-recovery-已创建积分
- aurora-mysql-cluster-audit-日志
- aurora-resources-protected-by-备份计划
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-删除-禁用
- backup-recovery-point-minimum-保留检查
- clb-desync-mode-check

- cloudformation-stack-drift-detection-检查
- cloudformation-stack-service-role-检查
- cloudformation-termination-protection-check
- cloudtrail-all-read-s3-data-event-check
- cloudtrail-all-write-s3-data-event-check
- cloudtrail-s3-bucket-access-logging
- cloudtrail-s3-bucket-public-access-prohibited
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-启用日志
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-已启用验证
- cmk-backing-key-rotation-已启用
- codebuild-project-environment-privileged-检查
- codebuild-project-logging-enabled
- codebuild-project-s3 个日志加密
- codebuild-report-group-encrypted-在休息时
- cognito-identity-pool-unauth-访问检查
- connect-instance-logging-enabled
- cw-loggroup-retention-period-检查
- datasync-task-logging-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-mongo-db-authentication-已启用
- dms-neptune-iam-authorization-已启用
- dms-redis-tls-enabled

- dms-replication-instance-multi-az 已启用
- dms-replication-not-public
- docdb-cluster-encrypted-in-交通
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-已创建积分
- dynamodb-resources-protected-by-备份计划
- dynamodb-table-deletion-protection-已启用
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-已创建积分
- ebs-resources-protected-by-备份计划
- ebs-snapshot-block-public-访问
- ebs-snapshot-public-restorable-检查
- ec2-已client-vpn-connection-log启用
- ec2-ebs-encryption-by-default
- ec2-已enis-source-destination-check启用
- ec2-imdsv2-check
- ec2-instance-launched-with-allowed-ami
- ec2-instance-managed-by-ssm
- ec2-已last-backup-recovery-point创建
- ec2-已加launch-templates-ebs-volume密
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2 resources-protected-by-backup-计划
- ec2-security-group-attached-to-eni
- ec2-stopped-instance

- ec2-vpn-connection-logging-enabled
- ecr-private-image-scanning-已启用
- ecr-private-lifecycle-policy-已配置
- ecr-private-tag-immutability-已启用
- ecr-repository-cmk-encryption-已启用
- ecs-capacity-provider-termination-检查
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-版本
- ecs-task-definition-efs-启用加密
- ecs-task-definition-linux-user-non-root
- ecs-task-definition-network-mode-not-host
- ecs-task-definition-user-for-host-mode-check
- ecs-task-definition-windows-user-non-admin
- efs-access-point-enforce-用户身份
- efs-automatic-backups-enabled
- efs-encrypted-check
- efs-filesystem-ct-encrypted
- efs-in-backup-plan
- efs-last-backup-recovery-已创建积分
- efs-mount-target-public-可访问
- efs-resources-protected-by-备份计划
- eip-attached
- eks-cluster-secrets-encrypted
- eks-cluster-supported-version
- eks-endpoint-no-public-访问
- eks-secrets-encrypted
- elasticache-automatic-backup-check-已启用
- elasticache-redis-cluster-automatic-备份检查

- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elastic-beanstalk-managed-updates-已启用
- elbv2-listener-encryption-in-transit
- elbv2--check predefined-security-policy-ssl
- elb-acm-certificate-required
- elb-custom-security-policy-ssl 检查
- elb-predefined-security-policy-ssl 检查
- emr-kerberos-enabled
- emr-master-no-public-ip
- event-data-store-cmk-启用加密
- fms-shield-resource-policy-检查
- fms-webacl-resource-policy-检查
- fms-webacl-rulegroup-association-检查
- fsx-last-backup-recovery-已创建积分
- fsx-ontap-deployment-type-检查
- fsx-openzfs-deployment-type-检查
- fsx-resources-protected-by-备份计划
- fsx-windows-deployment-type-检查
- glue-job-logging-enabled
- glue-ml-transform-encrypted-在休息时
- glue-spark-job-supported-版本
- guardduty-eks-protection-audit-已启用
- guardduty-enabled-centralized
- guardduty-lambda-protection-enabled
- guardduty-non-archived-findings
- guardduty-s3-protection-enabled
- iam-customer-policy-blocked-kms 动作
- iam-inline-policy-blocked-kms 动作
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-root-access-key-检查
- iam-server-certificate-expiration-检查
- iam-user-mfa-enabled
- iam-user-unused-credentials-检查
- incoming-ssh-disabled
- inspector-ec2-scan-enabled
- inspector-ecr-scan-enabled
- inspector-lambda-standard-scan-已启用
- instances-in-vpc
- kinesis-firehose-delivery-stream-已加密
- kinesis-stream-backup-retention-检查
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-用于删除
- lambda-function-public-access-禁止
- lambda-function-xray-enabled
- mariadb-publish-logs-to-云监视日志
- mfa-enabled-for-iam-控制台访问权限
- mq-cloudwatch-audit-log-已启用
- msk-cluster-public-access-已禁用
- msk-unrestricted-access-check
- multi-region-cloud-trail-已启用
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-关联
- netfw-stateless-rule-group-不为空
- netfw-subnet-change-protection-已启用
- nlb-logging-enabled

- no-unrestricted-route-to-igw
- opensearch-primary-node-fault-容忍
- opensearch-update-check
- rabbit-mq-supported-version
- rds-aurora-postgresql-logs到云端观察
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-检查
- rds-instance-subnet-igw-检查
- rds-in-backup-plan
- rds-last-backup-recovery-已创建积分
- rds-logging-enabled
- rds-mariadb-instance-encrypted在途中
- rds-mysql-instance-encrypted在途中
- rds-postgresql-logs-to-云观察
- rds-postgres-instance-encrypted在途中
- rds-resources-protected-by-备份计划
- rds-sqlserver-encrypted-in-交通
- rds-sql-server-logs到云端观察
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-multi-az-已启用
- redshift-cluster-subnet-group-多可用区
- redshift-default-admin-check
- redshift-require-tls-ssl
- redshift-serverless-default-admin-检查
- redshift-serverless-default-db-姓名检查
- redshift-serverless-namespace-cmk-加密
- redshift-unrestricted-port-access
- required-tags

- restricted-incoming-traffic
- 仅限 s3 access-point-in-vpc-
- s3 access-point-public-access-方块
- s3--account-level-public-access 区块-周期性
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- s3-已bucket-cross-region-replication启用
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-宽容
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-已bucket-server-side-encryption启用
- s3-bucket-ssl-requests-only
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-已last-backup-recovery-point创建
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-计划
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-密钥已配置
- sagemaker-endpoint-config-prod-实例计数
- sagemaker-notebook-instance-kms-密钥已配置
- sagemaker-notebook-instance-platform-版本
- sagemaker-notebook-no-direct-互联网接入
- secretsmanager-rotation-enabled-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk

- securityhub-enabled
- service-catalog-shared-within-组织
- service-vpc-endpoint-enabled
- ses-sending-tls-required
- sqs-queue-dlq-check
- sqs-queue-policy-full-访问检查
- ssm-automation-block-public-共享
- ssm-automation-logging-enabled
- ssm-document-not-public
- storagegateway-last-backup-recovery-已创建积分
- storagegateway-resources-protected-by-备份计划
- subnet-auto-assign-public-ip 已禁用
- transfer-connector-logging-enabled
- transfer-family-server-no-ftp
- virtualmachine-last-backup-recovery-已创建积分
- virtualmachine-resources-protected-by-备份计划
- vpc-endpoint-enabled
- vpc-flow-logs-enabled
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port-restriction-检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- workspaces-root-volume-encryption-已启用
- workspaces-user-volume-encryption-已启用

使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则

> **Important**
>
> 必须先创建并启动 Amazon Config 配置记录器，才能使用 Amazon CloudFormation 创建 Amazon Config 托管规则。有关更多信息，请参阅管理配置记录器。

对于支持的 Amazon Config 托管规则，您可以使用 Amazon CloudFormation 模板为账户创建规则或更新现有 Amazon CloudFormation 堆栈。堆栈是您作为单个单元配置和更新的相关资源的集合。在使用模板启动堆栈时，将为您创建 Amazon Config 托管规则。模板仅创建规则，而不创建其他 Amazon 资源。

> **Note**
>
> 在更新 Amazon Config 托管规则时，将针对最新更改来更新模板。要为规则保存特定版本的模板，请下载该模板并将其上传到您的 S3 存储桶。

有关使用 Amazon CloudFormation 模板的更多信息，请参阅《Amazon CloudFormation 用户指南》中的 Amazon CloudFormation 入门。

为 Amazon CloudFormation 托管规则启动 Amazon Config 堆栈

1. 转至 CloudFormation 控制台并创建新堆栈。
2. 对于 Specify template（指定模板）：
   - 如果您已下载模板，请选择 Upload a template file（上传模板文件），然后选择 Choose file（选择文件）以上传模板。
   - 您也可以选择 Amazon S3 URL，然后输入模板 URL。`http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template`

   > **Note**
   >
   > 规则标识符应写在 ALL_CAPS_WITH_UNDERSCORES 中。例如，应为 CLOUDWATCH_LOG_GROUP_ENCRYPTED 而不是 cloudwatch-log-group-encrypted。对于某些规则，规则标识符与规则名称不同。确保使用规则标识符。例如，restricted-ssh 的规则标识符为 INCOMING_SSH_DISABLED。
3. 选择下一步。
4. 对于 Specify stack details（指定堆栈详细信息），键入堆栈名并输入 Amazon Config 规则的参数值。例如，如果您使用的是 `DESIRED_INSTANCE_TYPE` 托管规则模板，则可以指定实例类型，例如“m4.large”。
5. 选择下一步。

6. 对于 Options，您可以创建标签或配置其他高级选项。这些操作不是必需的。
7. 选择下一步。
8. 对于 Review，验证模板、参数和其他选项是否正确。
9. 选择创建。将在几分钟内创建堆栈。您可以在 Amazon Config 控制台中查看创建的规则。

您可以使用模板为 Amazon Config 托管规则创建单个堆栈或更新您的账户中的现有堆栈。如果您删除堆栈，也将删除从该堆栈创建的托管规则。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的使用堆栈。

Amazon Config 自定义规则

Amazon Config 自定义规则是您从头开始创建的规则。有两种方法可以创建 Amazon Config 自定义规则：使用 Lambda 函数（Amazon Lambda 开发人员指南）和使用策略即代码语言 Guard（Guard GitHub 存储库）。

使用 Lambda 创建的 Amazon Config 自定义规则称为 Amazon Config 自定义 Lambda 规则，使用 Guard 创建的 Amazon Config 自定义规则称为 Amazon Config 自定义策略规则。

在使用自定义规则之前，请参阅 注意事项

Amazon Config 自定义策略规则

可以从 Amazon Config 控制台创建，也可以使用 Amazon Config 规则 API 创建使用 Guard 编写的规则。Amazon Config自定义策略规则允许您创建 Amazon Config 自定义规则，无需使用 Java 或 Python 开发 Lambda 函数来管理您的自定义规则。Amazon Config自定义策略规则由配置更改启动。有关 Guard 的更多信息，请参阅 Guard GitHub 存储库。

Amazon Config 自定义 Lambda 规则

自定义 Lambda 规则为您提供了选项，可以使用 Java 或 Python 为 Amazon Config 自定义规则创建 Lambda 函数。Lambda 函数是您上传到 Amazon 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 Amazon Config 规则关联，则在规则启动时 Amazon Config 会调用该函数。之后，Lambda 函数会评估由 Amazon 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《Amazon Lambda 开发人员指南》中的函数和事件源。

Amazon Config 自定义规则的格式差异

下表显示了 ConfigurationItem 数据类型和 Amazon Config 自定义规则字段的格式差异。

ConfigurationItem	Amazon Config 自定义规则
`version`	`configurationItemVersion`
`accountId`	`awsAccountId`
`arn`	`ARN`
`configurationItemMD5Hash`	`configurationStateMd5Hash`

主题

- 创建 Amazon Config 自定义策略规则
- 创建 Amazon Config 自定义 Lambda 规则
- 管理 Amazon Config 自定义 Lambda 规则的已删除资源

创建 Amazon Config 自定义策略规则

您可以通过、Amazon Web Services 管理控制台Amazon CLI 或 Amazon Config API 创建 Amazon Config 自定义策略规则。

添加 Amazon Config 自定义策略规则

Using the console

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在 Amazon Web Services 管理控制台 菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的 Amazon 区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon 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. 在指定规则类型页面上，选择使用 Guard 创建自定义规则。
6. 在配置规则页面上，通过完成以下步骤创建规则：
    a. 对于规则名称，键入一个唯一的规则名称。
    b. 对于描述，键入规则的描述。

c. 对于 Guard 运行时版本，为您的 Amazon Config 自定义策略规则选择运行时系统。

d. 对于规则内容，可以为其填充规则的 Guard 自定义策略。

e. 对于评估模式，请选择在资源创建和管理过程中 Amazon Config 何时评估您的资源。根据此规则，Amazon Config 可以在预置资源之前、预置资源之后或同时在这两个阶段评估资源配置。

i. 选择开启主动评估，以允许您在部署资源之前对资源的配置设置进行评估。

开启主动评估后，您可以使用 StartResourceEvaluation API 和 GetResourceEvaluationSummary API 来检查您在这些命令中指定的资源是否会被您所在区域的账户中的主动规则标记为 NON_COMPLIANT。

有关使用此命令的更多信息，请参阅使用 Amazon Config 规则评估您的资源。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 Amazon Config 托管规则列表。

ii. 选择开启侦查评估以评估您的现有资源的配置设置。

对于侦查评估，Amazon Config 自定义策略规则由配置更改启动。将预先选择以下选项。

- 资源 – 在创建、更改或删除与指定资源类型（或类型和标识符）匹配的资源时。
- 标签 – 在创建、更改或删除包含指定标签的资源时。
- 所有更改 – 在创建、更改或删除 Amazon Config 记录的资源时。

Amazon Config 在检测到与规则的范围匹配的资源发生更改时运行评估。您可以使用范围来限制哪些资源启动评估。否则，当配置后的资源发生变化时，就会启动评估。

f. 对于参数，如果您的规则包含参数，可以自定义所提供的键的值。参数是资源在被视为符合规则之前必须遵守的属性。

7. 在审核和创建页面上，查看您的所有选择，然后再将规则添加到您的。Amazon Web Services 账户

8. 查看完规则后，选择添加规则。

Using the Amazon CLI

使用 `put-config-rule` 命令。

`Owner` 字段应为。`CUSTOM_POLICY`Amazon Config 自定义策略规则需要以下附加字段：

- `Runtime`：Amazon Config 自定义策略规则的运行时系统。
- `PolicyText`：包含 Amazon Config 自定义策略规则逻辑的策略定义。
- `EnableDebugLogDelivery`：为 Amazon Config 自定义策略规则启用调试日志记录的布尔表达式。默认值为。`false`

Using the API Reference

使用 PutConfigRule 操作。

`Owner` 字段应为。`CUSTOM_POLICY`Amazon Config 自定义策略规则需要以下附加字段：

- `Runtime`：Amazon Config 自定义策略规则的运行时系统。
- `PolicyText`：包含 Amazon Config 自定义策略规则逻辑的策略定义。
- `EnableDebugLogDelivery`：为 Amazon Config 自定义策略规则启用调试日志记录的布尔表达式。默认值为。`false`

为 Amazon Config 自定义策略规则编写规则内容

通过 Amazon Config 自定义策略规则，您可以使用 Amazon CloudFormation Guard 的域特定语言（DSL）来评估资源配置。本主题提供了编写自定义策略规则的模式和最佳实践。

有关如何使用 Guard 编写规则的更多信息，请参阅《Amazon CloudFormation Guard 用户指南》中的编写 Guard 规则，以及 Guard GitHub 资源库中的 Amazon CloudFormation Guard 2.0's Modes of Operation。

基本规则结构

使用以下基本格式创建规则：

```
# Basic rule format
rule <rule_name> when
    resourceType == "<AWS::Service::Resource>" {
    # Evaluation clauses
}

# Example with filtering
let resources_of_type = Resources.*[ Type == 'AWS::Service::Resource' ]
rule check_resources when %resources_of_type !empty {
```

```
    %resources_of_type.configuration.property == expected_value
}
```

关键组件

configuration

包含资源配置的内容。

supplementaryConfiguration

包含资源配置的其他内容。Amazon Config 针对某些资源类型返回此字段，用于补充针对配置字段返回的信息。

resourceType

正在评估的 Amazon 资源类型。

resourceId

资源的 ID（例如，`sg-xxxxxx`）。

accountId

与资源关联的 12 位数字 Amazon Web Services 账户 ID。

常见模式

Status checks

```
let allowed_status = ['ACTIVE', 'RUNNING']
rule check_resource_status when
    resourceType == "AWS::Service::Resource" {
    configuration.status IN %allowed_status
}
```

Required properties

```
rule check_required_properties when
    resourceType == "AWS::Service::Resource" {
    configuration.propertyName exists
    configuration.propertyName is_string  # or is_list, is_struct
}
```

Query blocks

```
configuration.Properties {
    property1 exists
    property2 is_string
    property3 IN [allowed_value1, allowed_value2]
}
```

Conditional evaluation

```
when configuration.feature_enabled == true {
    configuration.feature_settings exists
    configuration.feature_settings is_struct
}
```

Custom messages

```
rule check_compliance when
    resourceType == "AWS::Service::Resource" {
    configuration.property == expected_value <<Custom error message explaining the
 requirement>>
}}
```

高级功能

Range checks

```
rule check_numeric_limits {
    # Inclusive range (lower_limit <= value <= upper_limit)
    configuration.value IN r[minimum_value, maximum_value]

    # Exclusive range (lower_limit < value < upper_limit)
    configuration.value IN r(exclusive_min, exclusive_max)

    # Left inclusive, right exclusive (lower_limit <= value < upper_limit)
    configuration.value IN r[minimum_value, exclusive_max)

    # Left exclusive, right inclusive (lower_limit < value <= upper_limit)
    configuration.value IN r(exclusive_min, maximum_value]
}
```

Combining conditions

```
# AND conditions (implicit through new lines)
condition_1
condition_2

# OR conditions (explicit)
condition_3 OR
condition_4
```

Chaining rules

```
rule check_prerequisites {
    configuration.required_setting exists
}

rule check_details when check_prerequisites {
    configuration.required_setting == expected_value
}
```

最佳实践

- 将变量与 `let` 语句结合使用来提高可读性。
- 使用命名规则块对相关检查进行分组。
- 包括描述性注释。
- 使用适当的运算符（`exists`、`is_string`、`is_list`）。
- 使用支持不区分大小写匹配的正则表达式模式。

示例：dynamodb-pitr-enabled

以下示例显示了 Amazon Config 托管规则 ??? 的 Amazon Config 自定义策略规则版本的策略定义。此规则检查 DynamoDB 表是否启用了时间点恢复。

```
# Check if DynamoDB tables have Point-in-Time Recovery enabled
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
```

```
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
    let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription.pointIn
    %pitr == "ENABLED" <<DynamoDB tables must have Point-in-Time Recovery enabled>>
}
```

创建 Amazon Config 自定义 Lambda 规则

您可以开发自定义规则，并使用 Amazon Lambda 函数将其添加至。Amazon Config

您可以将每个自定义规则与一个 Lambda 函数关联，其中包含用于评估您的 Amazon 资源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。Amazon Config

Amazon 规则开发套件（RDK）

Amazon 规则开发套件（RDK）旨在支持直观且高效的“合规即代码”工作流程。它简化了与部署由自定义 Lambda 函数支持的 Amazon Config 规则相关的大量重复性繁重工作，并提供了一套精简的“开发 - 部署 - 监控”迭代流程。

有关分步说明，请参阅Amazon 规则开发套件（RDK）文档。

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

Amazon Lambda 将执行函数来响应由 Amazon 服务发布的事件。用于 Amazon Config 自定义 Lambda 规则的函数收到一个由 Amazon Config 发布的事件，然后该函数使用从该事件接收以及它通过 Amazon 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 Amazon Lambda 函数中常见模式的信息，请参阅《Amazon Lambda 开发人员指南》中的编程模型。

Example Function for Evaluations Triggered by Configuration Changes

Amazon Config 检测到自定义规则范围内的资源发生配置更改时，会调用函数示例如下。

如果您使用 Amazon Config 控制台创建与类似此示例的函数关联的规则，请选择 Configuration changes（配置更改）作为触发器类型。如果您使用 Amazon Config API 或 Amazon CLI 创

建规则，请将 MessageType 属性设置为 ConfigurationItemChangeNotification 和 OversizedConfigurationItemChangeNotification。这些设置可使您的规则在每次 Amazon Config 生成配置项或资源更改导致过大配置项时触发。

此示例评估您的资源并检查实例是否匹配资源类型。AWS::EC2::Instance此规则在 Amazon Config 生成配置项或过大配置项通知时触发。

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// 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.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );
```

```
}

// 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.
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await 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.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
```

```
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is
 not compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

函数运作

本函数在运行时执行以下操作：

1. 此函数在 Amazon Lambda 将 `event` 对象传递给 `handler` 函数时运行。在此示例中，该函数接受可选 `callback` 参数，该参数用于向调用方返回信息。Amazon Lambda 还会传递一个 `context` 对象，其中包含函数在运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。

2. 此函数检查事件的 messageType 是配置项还是过大配置项，然后返回配置项。
3. 处理程序调用 isApplicable 函数来确定资源是否已删除。

> **Note**
>
> 报告已删除资源的规则应返回 NOT_APPLICABLE 的评估结果，以避免不必要的规则评估。

4. 处理程序调用 evaluateChangeNotificationCompliance 函数并传递 configurationItem 在事件中发布的 ruleParameters 和 Amazon Config 对象。

   函数首先评估资源是否为 EC2 实例。如果资源不是 EC2 实例，函数会返回 NOT_APPLICABLE 这一合规性值。

   然后，函数评估配置项中的 instanceType 属性是否与 desiredInstanceType 参数值一致。如果值相等，该函数将返回。COMPLIANT如果值不相等，该函数将返回。NON_COMPLIANT
5. 处理程序通过初始化 Amazon Config 对象来做好向 putEvaluationsRequest 发送评估结果的准备。该对象包含 Evaluations 参数，这一参数用于识别受评估资源的合规性结果、资源类型和 ID。putEvaluationsRequest 对象还包含来自事件的结果令牌，该令牌可标识 Amazon Config 的规则和事件。
6. 处理程序通过向 Amazon Config 客户端的 putEvaluations 方法传递对象来向 config 发送评估结果。

Example Function for Periodic Evaluations

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

如果您使用 Amazon Config 控制台创建与类似此示例的函数关联的规则，请选择 Periodic（定期）作为触发器类型。如果您使用 Amazon Config API 或 Amazon CLI 创建规则，请将 MessageType 属性设置为。ScheduledNotification

本示例会检查指定资源的总数是否超出指定的最大值。

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand,
 PutEvaluationsCommand } from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});
```

```
// Receives the event and context from AWS Lambda.
export const handler = async (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),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount,
 count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not
 compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
```

```
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } 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 the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource
 type.", null);
    }
    if (!maxCountIsInt) {
```

```
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count,
 callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
    return count;
}
```

函数运作

本函数在运行时执行以下操作：

1. 此函数在 Amazon Lambda 将 `event` 对象传递给 `handler` 函数时运行。在此示例中，该函数接受可选 `callback` 参数，该参数用于向调用方返回信息。Amazon Lambda 还会传递一个 `context` 对象，其中包含函数在运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。

2. 为计数指定类型的资源，处理程序会调用 `countResourceTypes` 函数，而且它传递其从事件收到的 `applicableResourceType` 参数。`countResourceTypes` 函数调用 `listDiscoveredResources` 客户端的 `config` 方法，该方法返回适用资源的标识符列表。该函数使用此列表的长度来确定适用资源的数量，而且它将此计数返回到处理程序。
3. 处理程序通过初始化 Amazon Config 对象来做好向 `putEvaluationsRequest` 发送评估结果的准备。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。Amazon Web Services 账户您可以使用 `Evaluations` 参数将结果应用于 Amazon Config 支持的任何资源类型。`putEvaluationsRequest` 对象还包含来自事件的结果令牌，该令牌可标识 Amazon Config 的规则和事件。
4. 在 `putEvaluationsRequest` 对象中，处理程序调用 `evaluateCompliance` 函数。此函数测试适用资源的数量是否超出分配给事件所提供的 `maxCount` 参数的最大值。如果资源的数量超出最大值，函数将返回。`NON_COMPLIANT`如果资源的数量没有超出最大值，函数将返回。`COMPLIANT`
5. 处理程序通过向 Amazon Config 客户端的 `putEvaluations` 方法传递对象来向 `config` 发送评估结果。

用于 Amazon Config 规则（Python）的示例 Amazon Lambda 函数

Amazon Lambda 将执行函数来响应由 Amazon 服务发布的事件。用于 Amazon Config 自定义 Lambda 规则的函数收到一个由 Amazon Config 发布的事件，然后该函数使用从该事件接收以及它通过 Amazon 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 Amazon Lambda 函数中常见模式的信息，请参阅《Amazon Lambda 开发人员指南》中的编程模型。

Example Function for Evaluations Triggered by Configuration Changes

Amazon Config 检测到自定义规则范围内的资源发生配置更改时，会调用函数示例如下。

如果您使用 Amazon Config 控制台创建与类似此示例的函数关联的规则，请选择 Configuration changes（配置更改）作为触发器类型。如果您使用 Amazon Config API 或 Amazon CLI 创建规则，请将 `MessageType` 属性设置为 `ConfigurationItemChangeNotification` 和 `OversizedConfigurationItemChangeNotification`。这些设置可使您的规则在每次 Amazon Config 生成配置项或资源更改导致过大配置项时触发。

```
import botocore
import boto3
```

```
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
```

```
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] =
 json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'],
 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')

# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
```

```
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
```

```
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

函数运作

本函数在运行时执行以下操作：

1. 此函数在 Amazon Lambda 将 `event` 对象传递给 `handler` 函数时运行。在此示例中，该函数接受可选 `callback` 参数，该参数用于向调用方返回信息。Amazon Lambda 还会传递一个 `context` 对象，其中包含函数在运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。
2. 此函数检查事件的 `messageType` 是配置项还是过大配置项，然后返回配置项。
3. 处理程序调用 `isApplicable` 函数来确定资源是否已删除。

> **Note**
>
> 报告已删除资源的规则应返回 `NOT_APPLICABLE` 的评估结果，以避免不必要的规则评估。

4. 处理程序调用 evaluateChangeNotificationCompliance 函数并传递 configurationItem 在事件中发布的 ruleParameters 和 Amazon Config 对象。

   函数首先评估资源是否为 EC2 实例。如果资源不是 EC2 实例，函数会返回 NOT_APPLICABLE 这一合规性值。

   然后，函数评估配置项中的 instanceType 属性是否与 desiredInstanceType 参数值一致。如果值相等，该函数将返回。COMPLIANT如果值不相等，该函数将返回。NON_COMPLIANT
5. 处理程序通过初始化 Amazon Config 对象来做好向 putEvaluationsRequest 发送评估结果的准备。该对象包含 Evaluations 参数，这一参数用于识别受评估资源的合规性结果、资源类型和 ID。putEvaluationsRequest 对象还包含来自事件的结果令牌，该令牌可标识 Amazon Config 的规则和事件。
6. 处理程序通过向 Amazon Config 客户端的 putEvaluations 方法传递对象来向 config 发送评估结果。

Example Function for Periodic Evaluations

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

如果您使用 Amazon Config 控制台创建与类似此示例的函数关联的规则，请选择 Periodic（定期）作为触发器类型。如果您使用 Amazon Config API 或 Amazon CLI 创建规则，请将 MessageType 属性设置为。ScheduledNotification

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
```

```
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission
 to assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value
 to the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
```

```
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled
 rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report
 on the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])
        valid_rule_parameters = evaluate_parameters(rule_parameters)
```

```
    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
count_resource_types(valid_rule_parameters['applicableResourceType'], '',
resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
ResultToken=event['resultToken'])
```

函数运作

本函数在运行时执行以下操作：

1. 此函数在 Amazon Lambda 将 `event` 对象传递给 `handler` 函数时运行。在此示例中，该函数接受可选 `callback` 参数，该参数用于向调用方返回信息。Amazon Lambda 还会传递一个 `context` 对象，其中包含函数在运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。
2. 为计数指定类型的资源，处理程序会调用 `countResourceTypes` 函数，而且它传递其从事件收到的 `applicableResourceType` 参数。`countResourceTypes` 函数调用 `listDiscoveredResources` 客户端的 `config` 方法，该方法返回适用资源的标识符列表。该函数使用此列表的长度来确定适用资源的数量，而且它将此计数返回到处理程序。
3. 处理程序通过初始化 Amazon Config 对象来做好向 `putEvaluationsRequest` 发送评估结果的准备。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。Amazon Web Services 账户您可以使用 `Evaluations` 参数将结果应用于 Amazon Config 支持的任何资源类型。`putEvaluationsRequest` 对象还包含来自事件的结果令牌，该令牌可标识 Amazon Config 的规则和事件。
4. 在 `putEvaluationsRequest` 对象中，处理程序调用 `evaluateCompliance` 函数。此函数测试适用资源的数量是否超出分配给事件所提供的 `maxCount` 参数的最大值。如果资源的数量超出最大值，函数将返回。`NON_COMPLIANT`如果资源的数量没有超出最大值，函数将返回。`COMPLIANT`

5. 处理程序通过向 Amazon Config 客户端的 `putEvaluations` 方法传递对象来向 `config` 发送评估结果。

Amazon Config 规则的示例事件

当触发规则时，Amazon Config 会通过发布一个事件来调用该规则的 Amazon Lambda 函数。然后，Amazon Lambda 会将事件传递到该函数的处理程序，从而执行该函数。

Example Event for Evaluations Triggered by Configuration Changes

Amazon Config当 检测到规则范围内的资源的配置更改时，它会发布一个事件。下面的示例事件演示规则被某个 EC2 实例的配置更改所触发。

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

Example Event for Evaluations Triggered by Oversized Configuration Changes

某些资源更改会生成过大配置项。下面的示例事件演示规则被某个 EC2 实例的过大配置更改所触发。

```
{
```

```
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

Example Event for Evaluations Triggered by Periodic Frequency

Amazon Config当 以您指定的频率（如每 24 小时）评估您的资源时，它会发布一个事件。下面的示例事件演示规则被定期频率触发。

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime
\":\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",
\"recordVersion\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

事件属性

Amazon Config 事件的 JSON 对象包含以下属性：

`invokingEvent`

触发规则评估的事件。如果事件是为了响应资源配置更改而发布的，则此属性的值是一个包含 JSON `configurationItem` 或 `configurationItemSummary`（对于过大配置项）的字符串。该配置项表示相关资源在 Amazon Config 检测到更改时的状态。有关配置项的示例，请参阅 `get-resource-config-history` 中的 Amazon CLI 查看配置历史记录 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 Amazon Config 控制台创建自定义 Lambda 规则时，您可以定义参数。您也可以使用 `InputParameters` `PutConfigRule` API 请求中的 Amazon Config 属性或 `put-config-rule` Amazon CLI 命令来定义参数。

参数的 JSON 代码包含在字符串中，因此，函数必须通过 JSON 解析程序解析字符串，以便能够评估其内容，如下面的 Node.js 示例中所示：

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

函数必须通过 Amazon Config 调用传递给 `PutEvaluations` 的令牌。

`eventLeftScope`

表明要评估的 Amazon 资源是否已从规则范围内删除的布尔值。如果值为，`true`则该函数表示可通过传递 `NOT_APPLICABLE` 作为 `ComplianceType` 调用中的 `PutEvaluations` 属性值来忽略评估。

`executionRoleArn`

分配给 Amazon Config 的 IAM 角色的 ARN。

`configRuleArn`

Amazon Config 分配给规则的 ARN。

`configRuleName`

您向导致 Amazon Config 发布事件并调用函数的规则分配的名称。

`configRuleId`

Amazon Config 分配给规则的 ID。

`accountId`

拥有规则的 Amazon Web Services 账户 的 ID。

`version`

Amazon 分配的版本号。如果 Amazon 向 Amazon Config 事件添加属性，则版本号会递增。如果函数需要仅在匹配或超过特定版本的事件中的属性，则该函数可以检查此属性的值。

Amazon Config 事件的当前版本为 1.0。

管理 Amazon Config 自定义 Lambda 规则的已删除资源

报告已删除资源的规则应返回 `NOT_APPLICABLE` 的评估结果，以避免不必要的规则评估。

删除资源时，Amazon Config 会创建一个 `configurationItemStatus` 为 `ResourceDeleted` 的。`configurationItem`您可以使用此元数据检查规则是否报告了已删除的资源。有关配置项的更多信息，请参阅概念 | 配置项。

包括以下代码段以检查是否有已删除的资源，如果报告了已删除的资源，则将 Amazon Config 自定义 Lambda 规则的评估结果设置为 `NOT_APPLICABLE`：

Custom Lambda Rules (Node.js)

```
// 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;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> 默认情况下，Amazon Config 托管规则和 Amazon Config 自定义策略规则会处理此行为。如果您将 Python 和 Amazon Config 开发工具包（RDK）与 Amazon Config 开发工具包库（RDKlib）结合使用来创建 Amazon Config 自定义 Lambd 规则，则导入的评估程序类将检查此行为。有关如何使用 RDK 和 RDKlib 编写规则的信息，请参阅使用 RDK 和 RDKlib 编写规则。

服务相关的 Amazon Config 规则

服务相关的 Amazon Config 规则是一种独特类型的 Amazon Config 托管规则，支持其他 Amazon 服务在您的账户中创建 Amazon Config 规则。服务相关的规则已预定义，以包含代表您调用其他 Amazon 服务所需的所有权限。这些规则类似于 Amazon 服务在您的 Amazon Web Services 账户中为合规性验证建议的标准。

这些服务相关的 Amazon Config 规则由 Amazon 服务团队拥有。Amazon 服务团队会在您的 Amazon Web Services 账户中创建这些规则。您具有对这些规则的只读访问权限。如果您已订阅这些规则链接到的 Amazon 服务，将无法编辑或删除这些规则。

服务相关规则和 Amazon Command Line Interface

使用 Amazon CLI 时，PutConfigRule、DeleteConfigRule 和 DeleteEvaluationResults API 返回访问被拒绝，并显示以下错误消息：

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

服务相关规则和 Amazon Config 控制台

在 Amazon Config 控制台中，服务相关的 Amazon Config 规则将显示在 Rules（规则）页面中。控制台中的编辑 和删除结果 按钮显示为灰色，以限制您编辑规则。您可以通过选择规则来查看规则的详细信息。

服务相关规则、修正操作和合规包

要向合规包中的服务相关规则添加修正操作，您需要将修正操作添加到合规包模板本身，然后使用更新的模板更新合规包。有关更新合规包的信息，请参阅部署合规包（控制台）、部署合规包（Amazon CLI）和管理组织合规包。

编辑和删除服务相关角色

要编辑或删除服务相关规则，请联系创建该规则的 Amazon 服务团队。例如，对于由 Amazon Security Hub CSPM 创建的服务相关规则，您可以按照《Amazon Security Hub CSPM 用户指南：禁用安全标准》中的以下步骤移除服务相关规则。

添加 Amazon Config 规则

您可以使用 Amazon Config 控制台或 Amazon SDKs 添加规则。

主题

- 添加规则（控制台）
- 添加规则 (Amazon SDKs)

添加规则（控制台）

规则页面在一个表中显示您的规则及其当前的合规性结果。每条规则的结果都是 “正在评估...” 直到根据规则 Amazon Config 完成对您的资源进行评估。您可以使用刷新按钮更新结果。 Amazon Config 完

成评估后，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 使用查看Amazon资源的合规信息和评估结果Amazon Config。

> **Note**
>
> 添加新规则时， Amazon Config 会评估资源清单中的适用资源，包括以前记录的资源。例如，如果您记录了`AWS::IoT::Policy`资源，但后来将其排除在记录范围之外，则 Amazon Config 会将初始配置项目 (CIs) 保留在清单中。尽管 CIs 当它们的关联资源类型被排除在记录之外时 Amazon Config 不再更新它们，但它会保留其上次录制的状态，并在您添加适用的规则时对其进行评估。
>
> Amazon Config 不评估不在资源清单中的资源。例如，如果您添加了???规则，但没有记录并且从未记录过`AWS::Amplify::Branch`资源，则 Amazon Config 无法评估您账户中的 Amazon Amplify 分支机构是合规还是不合规。
>
> 有关更多信息，请参阅 使用 Amazon Config 记录 Amazon 资源。

添加规则

添加一项规则

1. 登录 Amazon Web Services 管理控制台 并在家中打开https://console.aws.amazon.com/config/主 Amazon Config机。
2. 在 Amazon Web Services 管理控制台 菜单中，确认区域选择器设置为支持 Amazon Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon 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. 在指定规则类型页面上，通过完成以下步骤指定规则类型：
   a. 在搜索字段中键入内容，以便按规则名称、描述和标签筛选托管规则列表。例如，键入EC2返回评估 EC2 资源类型的规则，或者键入定期返回定期触发的规则。
   b. 您还可以创建自己的自定义规则。选择使用 Lambda 创建自定义规则或使用 Guard 创建自定义规则，然后按照创建自定义 Amazon Config Lambda 规则或创建 Amazon Config自定义策略规则中的步骤进行操作。
6. 在创建规则页面上，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. 对于描述，键入规则的描述。

c. 对于评估模式，请选择在资源创建和管理过程中何 Amazon Config 时评估您的资源。根据规则， Amazon Config 可以在部署资源之前、部署资源之后或两者兼而有之地评估您的资源配置。

i. 选择开启主动评估，以允许您在部署资源之前对资源的配置设置进行评估。

开启主动评估后，您可以使用 StartResourceEvaluationAPI 和 GetResourceEvaluationSummaryAPI 来检查您在这些命令中指定的资源是否会被您所在地区的账户中的主动规则标记为 “不合规”。

有关使用此命令的更多信息，请参阅使用 Amazon Config 规则评估您的资源。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 Amazon Config 托管规则列表。

ii. 选择开启侦查评估以评估您的现有资源的配置设置。

对于侦查评估，有两种类型的触发器：在配置发生更改时和定期。

A. 如果您的规则的触发器类型包括配置更改，请为 Amazon Config 调用您的 Lambda 函数的更改范围指定以下选项之一：

- 资源 – 在创建、更改或删除与指定资源类型（或类型和标识符）匹配的资源时。
- 标签 – 在创建、更改或删除包含指定标签的资源时。
- 所有更改-创建、更改或删除记录的资源时。 Amazon Config

Amazon Config 当它检测到与规则范围相匹配的资源发生变化时，就会运行评估。您可以使用范围来定义哪些资源启动评估。

B. 如果您的规则的触发器类型包括定期，请指定 Amazon Config 调用 Lambda 函数的频率。

d. 对于参数，如果您的规则包含参数，可以自定义所提供的键的值。参数是资源在被视为符合规则之前必须遵守的属性。

7. 在审核和创建页面上，查看您的所有选择，然后再将规则添加到您的。 Amazon Web Services 账户如果规则没有按预期运行，您可能会在合规性中看到以下内容之一：

- 未报告任何结果- Amazon Config 根据规则评估了您的资源。该规则不适用于其范围内的 Amazon 资源，指定的资源已被删除，或者评估结果被删除。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。

- 范围内没有资源- Amazon Config 无法根据此规则评估您记录的 Amazon 资源，因为您的所有资源都不在该规则的范围内。要获得评估结果，请编辑规则并更改其范围，或者使用 “设置” 页面添加 Amazon Config 要记录的资源。
- Evaluations failed（评估失败）- 有关可帮助您确定问题的信息，请选择规则名称以打开其详细信息页面并查看错误消息。

添加规则 (Amazon SDKs)

添加规则

以下代码示例演示如何使用 PutConfigRule。

CLI

Amazon CLI

添加 Amazon 托管 Config 规则

以下命令提供用于添加 Amazon 托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

RequiredTagsForEC2Instances.json 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
```

```
}
```

对于该ComplianceResourceTypes属性，此 JSON 代码将范围限制为该AWS::EC2::Instance类型的资源，因此 Amazon Config 将仅根据规则评估 EC2 实例。由于该规则是托管规则，因此 Owner 属性设置为，AWSSourceIdentifier 属性设置为规则标识符。REQUIRED_TAGS对于 InputParameters 属性，指定了规则所需的标签键 CostCenter 和 Owner。

如果命令成功， Amazon Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules命令并指定规则名称。

添加客户托管的 Config 规则

以下命令提供用于添加客户托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

InstanceTypesAreT2micro.json 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

对于该ComplianceResourceTypes属性，此 JSON 代码将范围限制为该AWS::EC2::Instance类型的资源，因此 Amazon Config 将仅根据规则评估 EC2 实例。由于此规则是客户托管规则，因此该Owner属性设置为CUSTOM_LAMBDA，并且该SourceIdentifier属性设置为 Lambda 函数 Amazon 的 ARN。SourceDetails对象为必填项。当 Confi Amazon g 调用 Amazon Lambda 函数根据规则评估资源时，为该InputParameters属性指定的参数将传递给 Lambda 函数。

如果命令成功， Amazon Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules命令并指定规则名称。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考PutConfigRule中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
 publicly
        readable.

        :param rule_name: The name to give the rule.
```

```
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅适用PutConfigRule于 Python 的Amazon SDK (Boto3) API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    " Create a config rule for S3 bucket public read prohibition
    lo_cfs->putconfigrule(
```

```
      io_configrule = NEW /aws1/cl_cfsconfigrule(
        iv_configrulename = iv_rule_name
        iv_description = |S3 Public Read Prohibited Bucket Rule|
        io_scope = NEW /aws1/cl_cfsscope(
          it_complianceresourcetypes = VALUE /aws1/
cl_cfscplncresrctypes_w=>tt_complianceresourcetypes(
            ( NEW /aws1/cl_cfscplncresrctypes_w( |AWS::S3::Bucket| ) )
          )
        )
        io_source = NEW /aws1/cl_cfssource(
          iv_owner = |AWS|
          iv_sourceidentifier = |S3_BUCKET_PUBLIC_READ_PROHIBITED|
        )
        iv_inputparameters = '{}'
        iv_configrulestate = |ACTIVE|
      )
    ).
    MESSAGE 'Created AWS Config rule.' TYPE 'I'.
```

- 有关 API 的详细信息，请参阅适用PutConfigRule于 S AP 的Amazon SDK ABAP API 参考。

更新 Amazon Config 规则

您可以使用 Amazon Config 控制台或 Amazon SDKs 更新规则。

主题

- 更新规则（控制台）
- 更新规则 (Amazon SDKs)

更新规则（控制台）

规则页面在一个表中显示您的规则及其当前的合规性结果。每条规则的结果都是 “正在评估...” 直到根据规则 Amazon Config 完成对您的资源进行评估。您可以使用刷新按钮更新结果。 Amazon Config 完成评估后，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 使用查看Amazon资源的合规信息和评估结果Amazon Config。

更新规则

更新规则

1. 登录 Amazon Web Services 管理控制台 并在家中打开https://console.aws.amazon.com/config/主 Amazon Config机。
2. 在 Amazon Web Services 管理控制台 菜单中，确认区域选择器设置为支持 Amazon Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 区域和终端节点。
3. 在左侧导航窗格中，选择 Rules。
4. 选择规则，然后为要更新的规则选择编辑规则。
5. 在编辑规则页面上修改设置，以根据需要更改您的规则。
6. 选择保存。

更新规则 (Amazon SDKs)

更新规则

如果要更新之前添加的规则，请在此请求中使用的 `ConfigRuleName` 数据类型中按、`ConfigRuleId``ConfigRuleArn` 或 `ConfigRule` 指定规则。您使用的 `PutConfigRule` 命令与添加规则时使用的命令相同。

以下代码示例演示如何使用 `PutConfigRule`。

CLI

Amazon CLI

添加 Amazon 托管 Config 规则

以下命令提供用于添加 Amazon 托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` 是一个包含规则配置的 JSON 文件：

```
{
```

```
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

对于该ComplianceResourceTypes属性，此 JSON 代码将范围限制为该AWS::EC2::Instance类型的资源，因此 Amazon Config 将仅根据规则评估 EC2 实例。由于该规则是托管规则，因此 Owner 属性设置为，AWSSourceIdentifier 属性设置为规则标识符。REQUIRED_TAGS对于 InputParameters 属性，指定了规则所需的标签键 CostCenter 和 Owner。

如果命令成功， Amazon Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules命令并指定规则名称。

添加客户托管的 Config 规则

以下命令提供用于添加客户托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

InstanceTypesAreT2micro.json 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
```

```
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

对于该ComplianceResourceTypes属性，此 JSON 代码将范围限制为该AWS::EC2::Instance类型的资源，因此 Amazon Config 将仅根据规则评估 EC2 实例。由于此规则是客户托管规则，因此该Owner属性设置为CUSTOM_LAMBDA，并且该SourceIdentifier属性设置为 Lambda 函数 Amazon 的 ARN。SourceDetails 对象为必填项。当 Confi Amazon g 调用 Amazon Lambda 函数根据规则评估资源时，为该InputParameters属性指定的参数将传递给 Lambda 函数。

如果命令成功， Amazon Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules命令并指定规则名称。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考PutConfigRule中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """
```

```
    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅适用PutConfigRule于 Python 的Amazon SDK (Boto3) API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    " Create a config rule for S3 bucket public read prohibition
    lo_cfs->putconfigrule(
      io_configrule = NEW /aws1/cl_cfsconfigrule(
        iv_configrulename = iv_rule_name
        iv_description = |S3 Public Read Prohibited Bucket Rule|
        io_scope = NEW /aws1/cl_cfsscope(
          it_complianceresourcetypes = VALUE /aws1/
cl_cfscplncresrctypes_w=>tt_complianceresourcetypes(
            ( NEW /aws1/cl_cfscplncresrctypes_w( |AWS::S3::Bucket| ) )
          )
        )
        io_source = NEW /aws1/cl_cfssource(
          iv_owner = |AWS|
          iv_sourceidentifier = |S3_BUCKET_PUBLIC_READ_PROHIBITED|
        )
        iv_inputparameters = '{}'
        iv_configrulestate = |ACTIVE|
      )
    ).
    MESSAGE 'Created AWS Config rule.' TYPE 'I'.
```

- 有关 API 的详细信息，请参阅适用PutConfigRule于 S AP 的Amazon SDK ABAP API 参考。

删除 Amazon Config 规则

您可以使用 Amazon Config 控制台或 Amazon SDKs 来删除您的规则。

主题

- 注意事项

- 删除规则（控制台）
- 删除规则 (Amazon SDKs)

注意事项

建议：在删除规则之前，请考虑将 **AWS::Config::ResourceCompliance** 资源类型排除在记录范围之外

删除规则会创建配置项目 (CIs)AWS::Config::ResourceCompliance，这可能会影响配置记录器的成本。如果您要删除评估大量资源类型的规则，则可能会导致 CIs 记录的资源数量激增。

为避免相关费用，您可以选择在删除规则之前禁用 AWS::Config::ResourceCompliance 资源类型的记录，并在删除规则后重新启用记录。

不过删除规则是一个异步过程，因此可能需要一个小时或更长时间才能完成。在对 AWS::Config::ResourceCompliance 禁用记录期间，将不会在关联资源的历史记录中记录规则评估。

删除规则（控制台）

规则页面在一个表中显示您的规则及其当前的合规性结果。每条规则的结果都是 “正在评估...” 直到根据规则 Amazon Config 完成对您的资源进行评估。您可以使用刷新按钮更新结果。 Amazon Config 完成评估后，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 使用查看Amazon资源的合规信息和评估结果Amazon Config。

> **Note**
>
> Amazon Config 仅评估其记录的资源类型。例如，如果您添加了启用 cloudtra il 的规则，但未记录 CloudTrail 跟踪资源类型，则 Amazon Config 无法评估您账户中的跟踪是合规还是不合规。有关更多信息，请参阅 使用 Amazon Config 记录 Amazon 资源。

删除规则

删除规则

1. 登录 Amazon Web Services 管理控制台 并在家中打开https://console.aws.amazon.com/config/主 Amazon Config机。

2. 在 Amazon Web Services 管理控制台 菜单中，确认区域选择器设置为支持 Amazon Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 区域和终端节点。
3. 在左侧导航窗格中，选择 Rules。
4. 从表中选择要删除的规则。
5. 从操作下拉列表中，选择删除规则。
6. 出现提示时，键入“Delete”（此条目区分大小写），然后选择删除。

删除规则 (Amazon SDKs)

删除规则

以下代码示例演示如何使用 `DeleteConfigRule`。

CLI

Amazon CLI

删除 C Amazon onfig 规则

以下命令删除名为的 Amazon Config 规则`MyConfigRule`：

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DeleteConfigRule中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
```

```
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅适用DeleteConfigRule于 Python 的Amazon SDK (Boto3) API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    lo_cfs->deleteconfigrule( iv_rule_name ).
    MESSAGE 'Deleted AWS Config rule.' TYPE 'I'.
```

- 有关 API 的详细信息，请参阅适用DeleteConfigRule于 S AP 的Amazon SDK ABAP API 参考。

查看 Amazon Config 规则的详细信息和合规性信息

> **Important**
>
> 要准确报告合规性状态，必须记录 `AWS::Config::ResourceCompliance` 资源类型。有关更多信息，请参阅录制 Amazon 资源。

您可以使用 Amazon Config 控制台或 Amazon SDKs 来查看您的规则。

主题

- 查看规则（控制台）
- 查看规则 (Amazon SDKs)

查看规则（控制台）

规则页面在一个表中显示您的规则及其当前的合规性结果。每条规则的结果都是“正在评估...”直到根据规则 Amazon Config 完成对您的资源进行评估。您可以使用刷新按钮更新结果。 Amazon Config 完成评估后，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 使用查看Amazon资源的合规信息和评估结果Amazon Config。

> **Note**
>
> Amazon Config 仅评估其记录的资源类型。例如，如果您添加了启用 cloudtra il 的规则，但未记录 CloudTrail 跟踪资源类型，则 Amazon Config 无法评估您账户中的跟踪是合规还是不合规。有关更多信息，请参阅 使用 Amazon Config 记录 Amazon 资源。

查看规则

查看您的规则

1. 登录 Amazon Web Services 管理控制台 并在家中打开https://console.aws.amazon.com/config/主Amazon Config机。

2. 在 Amazon Web Services 管理控制台 菜单中，确认区域选择器设置为支持 Amazon Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 区域和终端节点。
3. 在左侧导航窗格中，选择 Rules。
4. “规则” 页面显示您当前存在的所有规则 Amazon Web Services 账户。其中列出每条规则的名称、关联的修正操作和合规性状态。

   - 选择 Add rule 以开始创建规则。
   - 选择规则可查看其设置，或者选择规则，然后选择查看详细信息。
   - 当规则评估资源时，请查看规则的合规性状态。
   - 选择规则，然后选择编辑规则以更改该规则的配置设置，并为不合规的规则设置修正操作。

查看规则 (Amazon SDKs)

查看规则的详细信息

以下代码示例演示如何使用 `DescribeConfigRules`。

CLI

Amazon CLI

获取 Amazon Config 规则的详细信息

以下命令返回名为的 Amazon Config 规则的详细信息`InstanceTypesAreT2micro`：

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

输出：

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
```

```
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考[DescribeConfigRules](#)中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例列出账户的配置规则以及选定属性。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

输出：

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                  ------------
 -------------
 ---------------
```

```
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeConfigRules中的。

适用于 PowerShell V5 的工具

示例 1：此示例列出账户的配置规则以及选定属性。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

输出：

```
ConfigRuleName                                     ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                     ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                              config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required         config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeConfigRules中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- 有关 API 的详细信息，请参阅适用DescribeConfigRules于 Python 的Amazon SDK (Boto3) API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    DATA(lo_result) = lo_cfs->describeconfigrules(
      it_configrulenames = VALUE /aws1/
cl_cfsconfigrulenames_w=>tt_configrulenames(
        ( NEW /aws1/cl_cfsconfigrulenames_w( iv_rule_name ) )
      )
    ).
    ot_cfg_rules = lo_result->get_configrules( ).
    MESSAGE 'Retrieved AWS Config rule data.' TYPE 'I'.
```

- 有关 API 的详细信息，请参阅适用DescribeConfigRules于 S AP 的Amazon SDK ABAP API 参考。

查看规则的合规性信息

以下代码示例演示如何使用 `DescribeComplianceByConfigRule`。

CLI

Amazon CLI

获取您的 Amazon Config 规则的合规性信息

以下命令返回一个或多个 Amazon 资源违反的每个 Amazon Config 规则的合规性信息：

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

在输出中，每个 CappedCount 属性的值都表示有多少资源不符合相关规则。例如，以下输出表明 3 个资源不符合名为 InstanceTypesAreT2micro 的规则。

输出：

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DescribeComplianceByConfigRule中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例检索规则的合规性详细信息，该规则当前没有评估结果 ebs-optimized-instance，因此它返回 INSUFKIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

输出：

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

示例 2：此示例返回规则 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK 的不合规资源数量。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       2
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeComplianceByConfigRule中的。

适用于 PowerShell V5 的工具

示例 1：此示例检索规则的合规性详细信息，该规则当前没有评估结果 ebs-optimized-instance，因此它返回 INSUFKIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

输出：

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

示例 2：此示例返回规则 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK 的不合规资源数量。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       2
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeComplianceByConfigRule中的。

查看结果的合规性摘要

以下代码示例演示如何使用 GetComplianceSummaryByConfigRule。

CLI

Amazon CLI

获取您的 Amazon Config 规则的合规性摘要

以下命令返回合规和不合规的规则数量。

```
aws configservice get-compliance-summary-by-config-rule
```

在输出中，每个 CappedCount 属性的值都表示有多少规则合规或不合规。

输出：

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考GetComplianceSummaryByConfigRule中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例返回不合规的 Config 规则的数量。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       9
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetComplianceSummaryByConfigRule中的。

适用于 PowerShell V5 的工具

示例 1：此示例返回不合规的 Config 规则的数量。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       9
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetComplianceSummaryByConfigRule中的。

查看规则的评估结果

以下代码示例演示如何使用 GetComplianceDetailsByConfigRule。

CLI

Amazon CLI

获取 Amazon Config 规则的评估结果

以下命令返回所有不符合名为的 Amazon Config 规则的资源的评估结果InstanceTypesAreT2micro：

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

输出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考[GetComplianceDetailsByConfigRule](#)中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例获取规则的评估结果 access-keys-rotated并返回按合规类型分组的输出

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

输出：

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

示例 2：此示例查询合规资源的规则 access-keys-rotated的合规性详细信息。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

输出：

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetComplianceDetailsByConfigRule中的。

适用于 PowerShell V5 的工具

示例 1：此示例获取规则的评估结果 access-keys-rotated并返回按合规类型分组的输出

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

输出：

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

示例 2：此示例查询合规资源的规则 access-keys-rotated的合规性详细信息。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

输出：

```
ConfigRuleName      ResourceId            ResourceType
```

```
--------------      ----------          ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetComplianceDetailsByConfigRule中的。

为 Amazon Config 规则开启主动评估

使用 Amazon Config 控制台或 Amazon SDK 开启主动评估规则。有关支持主动评估的资源类型和托管规则列表，请参阅规则的组成部分 | 评估模式。

主题

- 开启主动评估（控制台）
- 开启主动评估（Amazon SDK）

开启主动评估（控制台）

规则页面在一个表中显示您的规则及其当前的合规性结果。在 根据规则完成对您的资源的评估前，每个规则的结果都显示为 Evaluating...Amazon Config。您可以使用刷新按钮更新结果。

当 Amazon Config 完成评估时，您可以看到合规或不合规的规则和资源类型。有关更多信息，请参阅使用查看Amazon资源的合规信息和评估结果Amazon Config

> **Note**
>
> Amazon 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，Amazon Config 将无法评估您账户中的跟踪是否合规。有关更多信息，请参阅 使用 Amazon Config 记录 Amazon 资源

开启主动评估

可以使用主动评估在资源部署之前对其进行评估。这使您可以根据您所在区域的账户中的主动规则集，评估一组资源属性（如果用于定义 Amazon 资源）是 COMPLIANT 还是 NON_COMPLIANT。

资源类型架构说明了资源的属性。您可以在 Amazon CloudFormation 注册表的“Amazon 公有扩展”中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的通过 Amazon CloudFormation 注册表管理扩展，以及 Amazon 资源和属性类型参考。

> **Note**
>
> 主动规则不会修复标记为 NON_COMPLIANT 的资源，也不会阻止部署这些资源。

开启主动评估

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在 Amazon Web Services 管理控制台菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关支持的 Amazon 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 区域和端点。
3. 在左侧导航窗格中，选择 Rules。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 Amazon Config 托管规则列表。
4. 选择规则，然后为要更新的规则选择编辑规则。
5. 对于评估模式，选择开启主动评估，以允许您在部署资源之前对资源的配置设置进行评估。
6. 选择保存。

开启主动评估后，您可以使用 StartResourceEvaluation API 和 GetResourceEvaluationSummary API 来检查您在这些命令中指定的资源是否会被您所在区域的账户中的主动规则标记为 NON_COMPLIANT。

例如，从 StartResourceEvaluation API 开始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
               --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                   "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 ResourceEvaluationId：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，将 ResourceEvaluationId 与 GetResourceEvaluationSummary API 结合使用来检查评估结果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

要查看有关评估结果的更多信息，例如哪条规则将资源标记为 NON_COMPLIANT，请使用 GetComplianceDetailsByResource API。

开启主动评估（Amazon SDK）

开启主动评估（Amazon CLI）

可以使用主动评估在资源部署之前对其进行评估。这使您可以根据您所在区域的账户中的主动规则集，评估一组资源属性（如果用于定义 Amazon 资源）是 COMPLIANT 还是 NON_COMPLIANT。

资源类型架构说明了资源的属性。您可以在 Amazon CloudFormation 注册表的“Amazon 公有扩展”中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的通过 Amazon CloudFormation 注册表管理扩展，以及 Amazon 资源和属性类型参考。

> **Note**
>
> 主动规则不会修复标记为 NON_COMPLIANT 的资源，也不会阻止部署这些资源。

开启主动评估

使用 put-config-rule 命令并为 EvaluationModes 启用。PROACTIVE

开启主动评估后，您可以使用 start-resource-evaluation CLI 命令和 get-resource-evaluation-summary CLI 命令检查您在这些命令中指定的资源是否会被您所在区域的账户中的主动规则标记为 NON_COMPLIANT。

例如，先使用 start-resource-evaluation 命令：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
               --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                   "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 ResourceEvaluationId：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，将 ResourceEvaluationId 和 get-resource-evaluation-summary 结合使用来检查评估结果：

```
aws configservice get-resource-evaluation-summary
```

```
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

要查看有关评估结果的更多信息，例如哪条规则将资源标记为 NON_COMPLIANT，请使用 get-compliance-details-by-resource CLI 命令。

> **Note**
>
> 有关支持主动评估的托管规则列表，请参阅按评估模式列出的 Amazon Config 托管规则列表。

开启主动评估（API）

可以使用主动评估在资源部署之前对其进行评估。这使您可以根据您所在区域的账户中的主动规则集，评估一组资源属性（如果用于定义 Amazon 资源）是 COMPLIANT 还是 NON_COMPLIANT。

资源类型架构说明了资源的属性。您可以在 Amazon CloudFormation 注册表的“Amazon 公有扩展”中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的通过 Amazon CloudFormation 注册表管理扩展，以及 Amazon 资源和属性类型参考。

> **Note**
>
> 主动规则不会修复标记为 NON_COMPLIANT 的资源，也不会阻止部署这些资源。

为规则开启主动评估

使用 PutConfigRule 操作并为 EvaluationModes 启用。PROACTIVE

开启主动评估后，您可以使用 StartResourceEvaluation API 和 GetResourceEvaluationSummary API 来检查您在这些命令中指定的资源是否会被您所在区域的账户中的主动规则标记为 NON_COMPLIANT。例如，从 StartResourceEvaluation API 开始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
               --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                   "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 ResourceEvaluationId：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，将 ResourceEvaluationId 与 GetResourceEvaluationSummary API 结合使用来检查评估结果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
```

```
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

要查看有关评估结果的更多信息，例如哪条规则将资源标记为 NON_COMPLIANT，请使用 GetComplianceDetailsByResource API。

> **Note**
>
> 有关支持主动评估的托管规则列表，请参阅按评估模式列出的 Amazon Config 托管规则列表。

向 Security Hub CSPM 发送规则评估

添加 Amazon Config 规则后，您还可以将规则评估发送到 Amazon Security Hub CSPM。与 Securit Amazon Config y Hub CSPM 之间的集成允许您对规则评估以及其他错误配置和安全问题进行分类和修复。

向 Security Hub CSPM 发送规则评估

要向 Security Hub CSPM 发送规则评估，必须先设置 Amazon Security Hub CSPM 和 Amazon Config，然后添加至少一条 Amazon Config 托管或自定义规则。之后， Amazon Config 立即开始向 Security Hub CSPM 发送规则评估。Security Hub CSPM 丰富了规则评估并将其转化为 Security Hub CSPM 调查结果。

有关此集成的更多信息，请参阅《 Amazon Security Hub CSPM 用户指南》中的可用 Amazon 服务集成。

使用 Amazon Config 规则评估资源

当您创建自定义规则或使用托管规则时，Amazon Config 按照这些规则评估您的资源。您可以按照您的规则对资源进行按需评估。例如，当您创建自定义规则，并且希望查看 Amazon Config 是否正确评估您的资源或确定 Amazon Lambda 函数的评估逻辑是否有问题时，这会很有用。

示例

1. 您创建一个自定义规则，用以评估您的 IAM 用户是否具有有效的访问密钥。
2. Amazon Config 按照您的自定义规则评估您的资源。
3. 在您的账户中存在一个没有有效访问密钥的 IAM 用户。您的规则不能正确将此资源标记为 NON_COMPLIANT。
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 NON_COMPLIANT。

向账户添加规则时，您可以指定在资源创建和管理过程中 Amazon Config 何时评估您的资源。资源创建和管理过程称为资源预置。您可以选择评估模式来指定在此过程中 Amazon Config 何时评估您的资源。

根据规则，Amazon Config 可以在部署资源之前、部署资源之后或同时在这两个阶段评估资源配置。在资源部署之前对其进行评估是主动评估。在资源部署之后对其进行评估是侦查评估。

主动模式

使用主动评估在资源部署之前对其进行评估。这使您可以根据您所在区域的账户中的主动规则集，评估一组资源属性（如果用于定义 Amazon 资源）是 COMPLIANT 还是 NON_COMPLIANT。

资源类型架构说明了资源的属性。您可以在 Amazon CloudFormation 注册表的“Amazon 公有扩展”中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅通过 Amazon CloudFormation 注册表管理扩展，以及《Amazon CloudFormation 用户指南》中的 Amazon 资源和属性类型参考。

> **Note**
>
> 主动规则不会修复标记为 NON_COMPLIANT 的资源，也不会阻止部署这些资源。

评估您的资源

开启主动评估

1. 登录到 Amazon Web Services 管理控制台，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在 Amazon Web Services 管理控制台菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的区域。有关支持的 Amazon 区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 区域和端点。
3. 在左侧导航窗格中，选择 Rules。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 Amazon Config 托管规则列表。
4. 选择规则，然后为要更新的规则选择编辑规则。
5. 对于评估模式，选择开启主动评估，以允许您在部署资源之前对资源的配置设置进行评估。
6. 选择保存。

> **Note**
>
> 您也可以使用 `put-config-rule` 命令并为 `EvaluationModes` 启用 `PROACTIVE`，或使用 PutConfigRule 操作并为 `EvaluationModes` 启用 `PROACTIVE` 来开启主动评估。

开启主动评估后，您可以使用 StartResourceEvaluation API 和 GetResourceEvaluationSummary API 来检查您在这些命令中指定的资源是否会被您所在区域的账户中的主动规则标记为 NON_COMPLIANT。

例如，从 StartResourceEvaluation API 开始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                    "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，将 `ResourceEvaluationId` 与 GetResourceEvaluationSummary API 结合使用来检查评估结果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

要查看有关评估结果的更多信息，例如哪条规则将资源标记为 NON_COMPLIANT，请使用 GetComplianceDetailsByResource API。

侦查模式

使用侦查评估来评估已部署的资源。这允许您评估现有资源的配置设置。

评估您的资源（控制台）

1. 登录到 Amazon Web Services 管理控制台，然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。

2. 在 Amazon Web Services 管理控制台菜单上，检查区域选择器是否设置为支持 Amazon Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 区域和终端节点。
3. 在导航窗格中，选择规则。规则页面显示每条规则的名称、关联的修正操作和合规性状态。
4. 从表中选择规则。
5. 从操作下拉列表中，选择重新评估。
6. Amazon Config 开始按照您的规则评估资源。

> **Note**
>
> 每分钟重新评估一次规则。您必须等待 Amazon Config 完成您的规则的评估，然后您才能开始另一个评估。如果规则同时被更新或同时被删除，您将无法运行评估。

评估您的资源 (CLI)

- 使用 start-config-rules-evaluation 命令：

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

Amazon Config 开始按照您的规则评估记录的资源配置。您还可以在请求中指定多个规则：

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

评估您的资源 (API)

使用 StartConfigRulesEvaluation 操作。

从 Amazon Config 规则中删除评估结果

在 Amazon Config 评估您的规则后，您可以在该规则的 Rules（规则）页或 Rules details（规则详细信息）页上查看评估结果。如果评估结果不正确，或者您要重新评估，您可以删除该规则的当前评估结果。例如，如果您的规则错误地评估您的资源或从您最近已从账户中删除资源，您可以删除评估结果，然后运行新的评估。

Deleting Evaluation Results (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 在 Amazon Web Services 管理控制台 菜单上，验证区域选择器是否设置为支持 Amazon Config 规则的 Amazon 区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 区域和终端节点。
3. 在导航窗格中，选择规则。规则页面显示每条规则的名称、关联的修正操作和合规性状态。
4. 从表中选择规则。
5. 从操作下拉列表中，选择删除结果。
6. 出现提示时，键入 Delete（此条目区分大小写），然后选择删除。删除评估后，您将无法对其进行检索。
7. 在评估结果被删除后，您可以手动开始新的评估。

Deleting Evaluation Results (CLI)

- 使用 delete-evaluation-results 命令。

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

  Amazon Config 删除规则的评估结果。

Deleting Evaluation Results (API)

使用 DeleteEvaluationResults 操作。

Amazon Config 规则疑难解答

如果您无法删除 Amazon Config 规则或收到类似于以下内容的错误，请检查以下问题进行故障排除：“出现错误” Amazon Config。

Amazon Identity and Access Management (IAM) 实体拥有 DeleteConfigRule该 API 的权限

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择用户或角色。
3. 选择用于删除 Amazon Config 规则的用户或角色，然后展开权限策略。

4. 在权限选项卡中，选择 JSON。
5. 在 JSON 预览窗格中，确认 IAM 策略是否允许使用该 DeleteConfigRuleAPI 的权限。

IAM 实体权限边界允许 DeleteConfigRule API

如果 IAM 实体有权限边界，请确保它允许 DeleteConfigRule API 的权限。

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择用户或角色。
3. 选择您用来删除 Amazon Config 规则的用户或角色，展开权限边界，然后选择 JSON。
4. 在 JSON 预览窗格中，确认 IAM 策略是否允许使用该 DeleteConfigRuleAPI 的权限。

> **Warning**
>
> IAM 用户具有长期凭证，这会带来安全风险。为帮助减轻这种风险，我们建议仅向这些用户提供执行任务所需的权限，并在不再需要这些用户时将其移除。

服务控制策略 (SCP) 允许 API DeleteConfigRule

1. https://console.aws.amazon.com/organizations/使用组织的管理账户打开 Amazon Organizations 控制台。
2. 在账户名中，选择 Amazon Web Services 账户
3. 在策略中，展开服务控制策略并记下附加的 SCP 策略。
4. 在页面的顶部，选择策略。
5. 选择策略，然后选择查看详细信息。
6. 在 JSON 预览窗格中，确认策略允许使用 DeleteConfigRuleAPI。

该规则是服务相关规则

启用安全标准后， Amazon Security Hub CSPM 会为您创建与服务相关的规则。您无法使用删除这些与服务相关的规则 Amazon Config，并且删除按钮显示为灰色。要删除服务相关规则，请参阅 Security Hub CSPM 用户指南中的禁用安全标准。

未进行任何修正操作

您无法删除正在执行修正操作的 Amazon Config 规则。按照步骤删除与该规则关联的修正操作。然后，再次尝试删除该规则。

> **Important**
>
> 仅删除处于失败或成功状态的修正操作。

使用修复不合规的资源 Amazon Config

Amazon Config 允许您修复由评估的不合规资源。 Amazon Config 规则 Amazon Config 使用Amazon Systems Manager 自动化文档应用补救。这些文档定义了要对由 Amazon Config 规则评估的不合规 Amazon 资源执行的操作。您可以使用 Amazon Web Services 管理控制台 或使用关联 SSM 文档。APIs

Amazon Config 提供了一组包含补救操作的托管自动化文档。您还可以创建自定义自动化文档并将其与 Amazon Config 规则关联。

主题

- 区域支持
- 为设置手动修复 Amazon Config
- 为设置自动修复 Amazon Config
- 正在删除的修复操作 Amazon Config

区域支持

目前，以下区域支持 Amazon Config 规则的修正操作：

区域名称	区域	端点	协议	
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
美国西部（北加利福尼亚）	us-west-1	config.us-west-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议	
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京）	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
中国（北京）	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS
中国（宁夏）	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

区域名称	区域	端点	协议	
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS	
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

为设置手动修复 Amazon Config

要对不合规的资源应用补救，您可以从预先填充的列表中选择要关联的修正操作，也可以使用 SSM 文档创建自己的自定义修复操作。 Amazon Config 中提供了建议的补救措施列表 Amazon Web Services 管理控制台。

Setting Up Manual Remediation (Console)

在中 Amazon Web Services 管理控制台，您可以选择通过将修复操作与规则关联来手动修复不合规的资源。 Amazon Config 借助所有修正操作，您可以选择手动或自动修正。

1. 登录 Amazon Web Services 管理控制台 并在家中打开https://console.aws.amazon.com/config/主 Amazon Config机。

2. 选择左侧的规则，然后在规则页面上，选择添加规则以向规则列表中添加新规则。

   对于现有规则，从规则列表中选择不合规规则，然后选择操作下拉列表。

3. 从操作下拉列表中，选择管理修正。选择“手动修正”，然后从建议列表中选择相应的修正操作。

   > **Note**
   >
   > 您只能管理非服务关联 Amazon Config 规则的修正。有关更多信息，请参阅服务相关的 Amazon 规则。

   根据所选的修正操作，您将会看到特定参数，或者看不到任何参数。

4. （可选）如果要将不合规资源的资源 ID 传递给修正操作，请选择 Resource ID parameter（资源 ID 参数）。如果选中，则在运行时会将该参数替换为要修正的资源的 ID。

   每个参数都具有静态值或动态值。如果未从下拉列表中选择特定资源 ID 参数，可以为每个键输入值。如果从下拉列表中选择资源 ID 参数，可以为除所选资源 ID 参数之外的所有其他键输入值。

5. 选择保存。此时将显示 Rules（规则）页面。

要对失败的修复操作进行故障排除，您可以运行 Amazon 命令行界面命令`describe-remediation-execution-status`来获取一组资源的修复执行的详细视图。详细信息包括修正执行步骤的状态、时间戳，以及失败步骤的任何错误消息。

Setting Up Manual Remediation (API)

使用以下 Amazon Config API 操作设置手动修复：

- PutRemediationConfigurations，使用带有选定目标或操作的特定 Amazon Config 规则添加或更新修正配置。
- StartRemediationExecution，根据上次已知的修正配置对指定 Amazon Config 规则运行按需修复。
- DescribeRemediationExecutionStatus，提供了一组资源的修正执行的详细视图，包括状态、执行修正步骤的时间戳以及失败步骤的任何错误消息。
- DescribeRemediationConfigurations，返回一个或多个修复配置的详细信息。

为设置自动修复 Amazon Config

要对不合规的资源应用补救，您可以从预先填充的列表中选择要关联的修正操作，也可以使用 SSM 文档创建自己的自定义修复操作。 Amazon Config 中提供了补救措施的列表 Amazon Web Services 管理控制台。

Setting Up Auto Remediation (Console)

在中 Amazon Web Services 管理控制台，您可以选择通过将修复操作与规则关联来自动修复不合规的资源。 Amazon Config 借助所有修正操作，您可以选择手动或自动修正。

1. 登录 Amazon Web Services 管理控制台 并在家中打开https://console.aws.amazon.com/config/主 Amazon Config机。
2. 选择左侧的规则，然后在规则页面上，选择添加规则以向规则列表中添加新规则。

   对于现有规则，从规则列表中选择不合规规则，然后选择操作下拉列表。
3. 从操作下拉列表中，选择管理修正。选择“自动修正”，然后从列表中选择相应的修正操作。

   > **Note**
   >
   > 您只能管理非服务关联 Amazon Config 规则的修正。有关更多信息，请参阅服务相关的 Amazon 规则。

   根据所选的修正操作，您将会看到特定参数，或者看不到任何参数。
4. 选择 Auto remediation（自动修正）以自动修正不合规的资源。

   如果在自动修正后资源仍然不合规，则可以设置规则以再次尝试自动修正。输入所需的重试次数和秒数。

   > **Note**
   >
   > 多次运行修正脚本会有关联的成本。只有当修正失败，并且在指定时间段内有效时才会重试；例如，在 300 秒内重试 5 次。有关更多信息，请参阅 Systems Manager Automation 定价。
5. （可选）如果要将不合规资源的资源 ID 传递给修正操作，请选择 Resource ID parameter（资源 ID 参数）。如果选中，则在运行时会将该参数替换为要修正的资源的 ID。

每个参数都具有静态值或动态值。如果未从下拉列表中选择特定资源 ID 参数，可以为每个键输入值。如果从下拉列表中选择资源 ID 参数，可以为除所选资源 ID 参数之外的所有其他键输入值。

6. 选择保存。此时将显示 Rules（规则）页面。

用于故障排除失败的修正措施

要对失败的修复操作进行故障排除，您可以运行 Amazon 命令行界面命令`describe-remediation-execution-status`来获取一组资源的修复执行的详细视图。详细信息包括修正执行步骤的状态、时间戳，以及失败步骤的任何错误消息。

即使是合规资源也可以启动自动修正

如果您使用 PutRemediationConfigurationsAPI 或 Amazon Config 控制台为特定 Amazon Config 规则启用自动修复，则会针对该特定规则的所有不合规资源启动修复流程。自动修正过程依赖于定期捕获的合规性数据快照。对于在快照计划之间更新的任何不合规资源，都将继续根据上次已知的合规性数据快照进行修正。

这意味着，在某些情况下，即使是合规资源也可以启动自动修正，因为引导处理器使用的数据库可能基于上次已知的合规性数据快照得出过时的评估结果。

Setting Up Auto Remediation (API)

使用以下 Amazon Config API 操作来设置自动修复：

- PutRemediationExceptions，使用特定 Amazon Config 规则为特定资源添加新的异常或更新现有例外。
- DescribeRemediationExceptions，返回一个或多个修正异常的详细信息。

正在删除的修复操作 Amazon Config

您可以使用 Amazon Config 控制台或 Amazon CLI 删除修复操作。

Deleting remediation actions (Console)

1. 登录 Amazon Web Services 管理控制台 并在家中打开https://console.aws.amazon.com/config/主 Amazon Config机。
2. 选择左侧的规则，然后在规则页面上，从规则列表中选择规则，再选择查看详细信息。

3. 在该*name of the rule*页面上，转到“修复操作”部分。展开这部分以查看更多详细信息。
4. 在修正操作部分中，选择删除并确认您的删除操作。

> **Note**
>
> 如果正在进行修正，修正操作不会被删除。如果选择删除修正操作，您将无法检索修正操作。删除修正操作不会删除关联的规则。

如果删除了修正操作，则资源 ID 参数将为空并显示“不适用”。在规则页面上，修正操作列将显示未设置关联规则。

Deleting remediation actions (API)

使用以下 Amazon Config API 操作来设置自动修复：

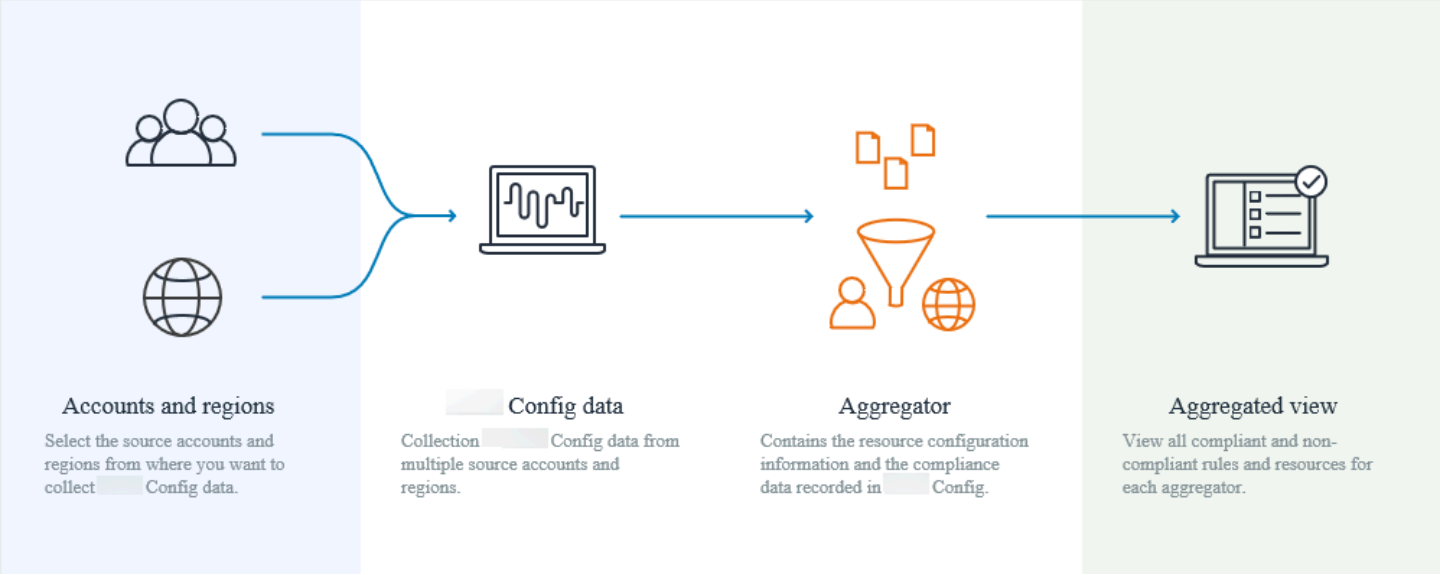
- DeleteRemediationConfiguration，删除修正配置。
- DeleteRemediationExceptions，删除资源密钥中提及的一个或多个修正异常。

多账户多区域数据聚合 Amazon Config

聚合器是一种从以下来源收集 Amazon Config 配置和合规性数据的 Amazon Config 资源类型：

- 多个账户和多个 Amazon 区域。
- 单个账户和多个 Amazon 区域。
- 一个组织中的一个组织 Amazon Organizations 以及该组织中所有已 Amazon Config 启用的账户。

使用聚合器查看在 Amazon Config中记录的资源配置和合规性数据。下图显示了聚合器如何从多个账户和地区收集 Amazon Config 数据。



应用场景

- 合规性监控：您可以聚合合规性数据，以评估组织或不同账户和区域的整体合规状况。
- 变更跟踪：您可以跟踪组织内或不同账户和地区的资源随时间发生的变化。
- 资源关系：您可以分析整个组织或不同账户和区域的资源依赖项和关系。

> **Note**
>
> 聚合器通过将数据从源账户复制到聚合器账户，提供源账户和聚合器有权查看的区域的只读视图。聚合器不提供对源账户或区域的可变访问权限。例如，这意味着您不能通过聚合器部署规则，也不能通过聚合器将快照文件推送到源账户或区域。

使用聚合器不会产生任何额外费用。

术语

源账户是您要 Amazon Web Services 账户 从中汇总 Amazon Config 资源配置和合规性数据的账户。源账户可以是 Amazon Organizations中的个人账户或组织。您可以单独提供源帐户，也可以通过它们进行检索 Amazon Organizations。

来源区域是您要从中汇总 Amazon Config 配置和合规性数据的 Amazon 区域。

聚合器账户 是您在其中创建聚合器的账户。

授权是指您向聚合器账户和地区授予的收集 Amazon Config 配置和合规性数据的权限。如果要聚合的源账户是 Amazon Organizations的一部分，则不需要授权。

服务相关聚合器与特定聚合器相关联。 Amazon Web Services 服务范围内的配置和合规性数据由相关服务设置。

区域支持

目前，多账户多区域数据聚合在以下区域中受支持：

区域名称	区域	端点	协议	
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
美国西部（北加利福尼亚）	us-west-1	config.us-west-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
亚太地区（马来西亚）	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（新西兰）	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（台北）	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
亚太地区（泰国）	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
亚太地区（东京）	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
中国（北京）	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS
中国（宁夏）	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS

区域名称	区域	端点	协议	
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
墨西哥（中部）	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS	
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议	
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

在 Amazon Config 聚合器控制面板中查看合规性和清单数据

聚合器页面上的控制面板显示您的聚合 Amazon 资源的配置数据。这些数据概述了您的规则、合规包及其合规状态。

此控制面板提供 Amazon 资源的总资源数量。资源类型和源账户按最大数量的资源排列。还提供合规和不合规规则以及合规包的计数。不合规规则按不合规资源的最大数量进行排名。不合规的合规包和源账户按不合规规则的最大数量进行排名。

设置后，Amazon Config 便会开始将指定源账户中的数据聚合到聚合器中。显示规则的合规性状态可能需要几分钟时间。

使用聚合器控制面板

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 导航到聚合器页面。您可以查看：
   - 您的规则及其合规性状态。
   - 您的合规包及其合规性状态。
   - 您的 Amazon 资源及其配置数据。
3. 从控制面板中选择聚合器。按聚合器名称筛选聚合器。您可以查看以下小组件：
   - 资源清单

     按资源计数降序查看所选聚合器中排名前 10 的资源类型。选择所选聚合器的资源总数（显示在资源清单后的括号中），以转到聚合资源页面，您可以在此页面上查看聚合器的所有资源。或者，也可以在小组件中选择一种资源类型，以转到使用指定资源类型筛选的聚合资源页面。

- 按资源计数列出的账户

  按资源计数降序查看所选聚合器中排名前 5 的资源类型。在小组件中选择一个账户，以进入使用指定账户筛选的资源页面。

- 不合规规则

  按照不合规资源的数量降序查看所选聚合器中排名前 5 的不合规规则。在小组件中选择一条规则，以进入指定规则的详细信息页面。选择查看所有不合规规则，以转至聚合规则页面，您可以在此页面上查看聚合器的所有规则。

- 按不合规规则列出的账户

  按照不合规规则的数量降序查看所选聚合器中排名前 5 的账户。在小组件中选择一个账户，以进入聚合规则页面，您可以在此页面上查看使用指定账户筛选的聚合器的所有规则。

- 按不合规的合规包列出的账户

  按照不合规的合规包数量降序查看所选聚合器中排名前 5 的账户。在小组件中选择一个账户，以进入聚合规则页面，您可以在此页面上查看使用指定账户筛选的聚合器的所有合规包。

4. 在左侧导航窗格中，从下拉菜单中选择下列选项之一：

   - 合规性控制面板

     使用汇总聚合器内资源合规性见解的小组件查看自动合规性控制面板。您可以查看数据，例如按不合规资源列出的排名前 10 的资源类型，以及按不合规规则列出的排名前 10 的账户级合规包。有关这些图形和图表的信息，请参阅合规性控制面板。

   - 合规包

     查看在聚合器中创建并关联到不同 Amazon Web Services 账户的所有合规包。合规包页面显示一个表，其中列出每个合规包的名称、区域、账户 ID 和合规性状态。您可以在此页面中选择合规包，还可以查看详细信息，以了解有关其规则和资源及其合规性状态的更多信息。

   - 规则：

     查看在聚合器中创建并关联到不同 Amazon 账户的所有规则。规则页面显示一个表，其中列出每条规则的名称、合规性状态、区域和账户。您可以在此页面中选择规则，还可以查看详细信息，以了解有关其聚合器、区域、账户 ID 和范围内资源的信息。

   - 清单控制面板

使用汇总聚合器内资源配置数据见解的小组件查看自动清单控制面板。您可以查看一些数据，例如，按资源计数排名前 10 的资源类型，以及按资源计数排名前 10 的账户。有关这些图形和图表的信息，请参阅清单控制面板。

- 资源。

  查看在聚合器中记录并关联到不同 Amazon 账户的所有资源。在资源页面中选择一个资源，然后选择查看详细信息，以查看其详细信息、与之关联的规则，以及当前的资源配置。您还可以查看有关资源的信息，例如其聚合器、区域、账户 ID、资源名称、资源类型和资源 ID。

- 授权

  查看并管理当前已授权或待授权的所有账户。在授权页面中，选择添加授权以提供对其他账户的访问权限。选择删除授权以撤消账户 ID 的访问权限。

> **Note**
>
> 故障排查
> 由于以下原因，您可能会在聚合视图中看到从所有源账户和区域收集的数据不完整消息：
>
> - Amazon 资源的不合规 Amazon Config 规则和配置数据正在传输中。
> - Amazon Config 无法找到符合所用筛选条件的规则。选择适当的账户或区域，然后重试。
>
> 您可能会在聚合视图中看到以下消息：从您的组织收集的数据不完整。您只能查看 24 小时的以下数据。显示此消息是由于以下原因：
>
> - 由于 IAM 角色无效，Amazon 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，Amazon Config 将会删除整个组织的数据。
> - Amazon Config 服务访问在您的组织中处于禁用状态。

合规性控制面板

使用汇总聚合器内资源合规性见解的小组件查看自动合规性控制面板。此控制面板只显示具有合规性结果的规则。

> **Note**
>
> 限制
> 合规性控制面板中的见解由 Amazon Config 的高级查询功能提供，此功能不支持嵌套结构或解开嵌套数组。这意味着合规性控制面板显示的是资源的总体合规性，而不是报告资源的每条特定规则的合规性状态。
> 例如，如果您检查资源类型 `AWS::Config::ResourceCompliance` 的配置项（CI），控制面板将显示报告该资源的所有规则的合规性结果。如果有 10 条规则报告该资源，其中 9 条为 COMPLIANT，只有 1 条为 NON_COMPLIANT，则该资源的总体合规性将为 NON_COMPLIANT。

按资源列出的合规性摘要

显示一个饼图，将选定聚合器的合规资源数量与不合规资源的数量进行比较。将鼠标悬停在图表上可查看合规资源和不合规资源的确切数量和百分比。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按不合规资源列出的排名前 10 的资源类型

显示一个水平条形图，按不合规资源数量降序比较选定聚合器中最多 10 种资源类型。将鼠标悬停在图表上，可查看每种资源类型不合规资源的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按不合规资源列出的排名前 10 的账户

按不合规资源列出的排名前 10 的账户显示一个水平条形图，按不合规资源数量降序比较选定聚合器中最多 10 个账户。将鼠标悬停在图表上，可查看每个账户不合规资源的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按不合规资源列出的排名前 10 的区域

显示一个水平条形图，按不合规资源数量降序比较选定聚合器收集数据的最多 10 个区域。将鼠标悬停在图表上，可查看每个区域不合规资源的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置。

按不合规规则列出的排名前 10 的账户级别合规包

显示一个水平条形图，按不合规规则数量降序比较选定聚合器中最多 10 个账户级别合规包。将鼠标悬停在图表上，可查看每个账户级别合规包的合规规则和不合规规则百分比。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按不合规规则列出的排名前 10 的组织级别合规包

显示一个水平条形图，按不合规规则数量降序比较选定聚合器中最多 10 个组织级别合规包。将鼠标悬停在图表上，可查看每个组织级别合规包的合规规则和不合规规则百分比。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按合规包中不合规规则列出的排名前 10 的账户

按合规包中不合规规则列出的排名前 10 的账户显示一个水平条形图，按所有合规包中不合规资源数量降序比较选定聚合器中最多 10 个账户。将鼠标悬停在图表上，可查看每个账户中不合规规则的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

清单控制面板

使用汇总聚合器内资源配置数据见解的小组件查看自动清单控制面板。

按资源计数列出的排名前 10 的资源类型

显示一个水平条形图，按资源计数降序比较选定聚合器中最多 10 种资源类型。将鼠标悬停在图表上，可查看每种资源类型的确切资源数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按区域列出的资源计数

显示一个水平条形图，按资源计数降序比较选定聚合器收集数据的最多 10 个区域。将鼠标悬停在图表上，可查看每个区域的确切资源数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置。

按资源计数列出的排名前 10 的账户

显示一个水平条形图，按资源计数降序比较选定聚合器中最多 10 个账户。将鼠标悬停在图表上，可查看每种资源类型的确切资源数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按 Amazon EC2 服务资源类型列出的资源计数

显示一个水平条形图，按资源计数降序比较选定聚合器中的 Amazon EC2 资源类型。将鼠标悬停在图表上，可查看每种 Amazon EC2 资源类型的确切资源数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。要使用此图表，您必须将记录器配置为记录 Amazon EC2 资源类型。有关更多信息，请参阅选择 Amazon Config 将记录的资源。

使用的排名前 10 的 EC2 实例类型

显示一个水平条形图，按使用情况降序比较选定聚合器中最多 10 个 Amazon EC2 实例类型。将鼠标悬停在图表上，可查看每种 EC2 实例类型的使用情况。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。要使用此图表，您必须将记录器配置为记录 EC2 实例资源类型。有关更多信息，请参阅记录 Amazon 资源。

按卷类型和大小列出的 EBS 卷计数

显示一个垂直条形图，按资源计数比较选定聚合器中的 EBS 卷。将鼠标悬停在图表上，可查看每种类型的 EBS 卷的计数和大小明细。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。要使用此图表，您必须将记录器配置为记录 EC2 卷资源类型。有关更多信息，请参阅选择 Amazon Config 将记录的资源。

按类型列出的正在运行的 EC2 实例数量与已停止的 EC2 实例数量

显示一个水平条形图，按实例类型比较选定聚合器中正在运行的 EC2 实例类型与已停止的 EC2 实例。将鼠标悬停在图表上，可查看每种类型已停止的 EC2 实例和正在运行的 EC2 实例的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。要使用此图表，您必须将记录器配置为记录 EC2 实例资源类型。有关更多信息，请参阅记录 Amazon 资源。

为 Amazon Config 创建聚合器

您可以使用 Amazon Config 控制台或 Amazon CLI 创建聚合器。您可以从 Amazon Config 中选择添加单个账户 ID 或添加我的组织来聚合数据。对于，Amazon CLI有两种不同的程序。

Creating Aggregators (Console)

在聚合器页面上，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。

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 导航到聚合器页面，然后选择创建聚合器。
3. 允许数据复制，授予 Amazon Config 权限，使其可将数据从源账户复制到聚合器账户中。

   选择允许 Amazon Config 将数据从源账户复制到聚合器账户。您须选中此复选框，才能继续添加聚合器。
4. 对于聚合器名称，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. 对于选择源账户，选择添加单个账户 ID 或添加我的组织来聚合数据。

   > **Note**
   > 使用添加单个账户 ID 来选择源账户时，需要获得授权。

   - 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. 选择添加 Amazon Web Services 账户 ID 以手动添加逗号分隔的 Amazon Web Services 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。

        或

        选择上传文件以上传逗号分隔的 Amazon Web Services 账户 ID 文件（.txt or .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**
>
> 您必须登录到管理账户或注册的委派管理员，并且所有功能都必须在组织中处于启用状态。如果调用者是管理账户，Amazon Config 会调用 `EnableAwsServiceAccess` API 以启用 Amazon Config 和 Amazon Organizations 之间的集成。如果调用者是注册的委派管理员，Amazon Config 会调用 `ListDelegatedAdministrators` API 来验证调用者是否是有效的委派管理员。
>
> 在委派管理员创建聚合器之前，请确保管理账户为委派管理员注册了 Amazon Config 服务主体名称（config.amazonaws.com）。要注册委派管理员，请参阅 注册 Amazon Config 的委托管理员

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

1. 选择从您的账户选择一个角色，以选择现有 IAM 角色。

> **Note**
>
> 在 IAM 控制台中，将 `AWSConfigRoleForOrganizations` 托管策略附加到您的 IAM 角色。附加此策略将允许 Amazon Config 调用 Amazon Organizations、`DescribeOrganizationListAWSServiceAccessForOrganizatio`n 和 `ListAccounts` API。默认情况下，`config.amazonaws.com` 会被自动指定为可信实体。

2. 或者，选择创建角色，然后键入 IAM 角色名称以创建 IAM 角色。

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。Amazon Web Services 区域
   - 选择包括未来的，Amazon Web Services 区域以从启用了多账户多区域数据聚合的所有未来 Amazon Web Services 区域中聚合数据。
7. 选择 Save（保存）。Amazon Config 将显示聚合器。

Creating Aggregators using Individual Accounts (Amazon CLI)

1. 打开命令提示符或终端窗口。
2. 输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输入以下内容之一。

- 以逗号分隔的您要为其聚合数据的 Amazon Web Services 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 Amazon Web Services 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:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
```

```
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

Creating Aggregators using Amazon Organizations (Amazon CLI)

在开始本过程之前，您必须先登录到管理账户或注册的委派管理员，并且所有功能都必须在组织中处于启用状态。

> **Note**
>
> 在委派管理员创建聚合器之前，请确保管理账户使用以下两个 Amazon Config 服务主体名称（`config.amazonaws.com` 和 `config-multiaccountsetup.amazonaws.com`）注册了委派管理员。要注册委派管理员，请参阅 注册 Amazon Config 的委托管理员

1. 打开命令提示符或终端窗口。
2. 如果尚未为 Amazon Config 聚合器创建 IAM 角色，请输入以下命令：

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid\":\"\",\"Effect
\":\"Allow\",\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action
\":\"sts:AssumeRole\"}]}" --description "Role for organizational AWS Config
 aggregator"
```

> **Note**
>
> 从此 IAM 角色复制 Amazon 资源名称（ARN），以便在您创建 Amazon Config 聚合器时使用。您可以在响应对象上找到 ARN。

3. 如果尚未为您的 IAM 角色附加策略，请附加 AWSConfigRoleForOrganizations 托管策略或输入以下命令：

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17",       "Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAW
```

4. 输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}"
```

5. 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:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

注册 Amazon Config 的委托管理员

委派管理员是给定 Amazon 组织内被授予指定 Amazon 服务的额外管理权限的账户。有关更多信息，请参阅《Amazon Organizations 用户指南》中的委托管理员。您必须使用 Amazon CLI 注册委托管理员。

注册委托管理员

1. 使用管理账户凭证登录。
2. 打开命令提示符或终端窗口。

3. 输入以下命令，以委派管理员身份为组织启用服务访问权限，以便在整个组织中部署和管理 Amazon Config 规则和合规包：

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. 输入以下命令，以委派管理员身份为组织启用服务访问权限，以聚合整个组织中的 Amazon Config 数据：

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. 要检查启用服务访问权限是否已完成，请输入以下命令并按 Enter 执行此命令。

```
aws organizations list-aws-service-access-for-organization
```

您应该可以看到类似于如下所示的输出内容：

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. 接下来，输入以下命令以注册一个成员账户作为 Amazon Config 的委派管理员。

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

以及

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. 要检查委派管理员注册是否已完成，请从管理账户中输入以下命令，然后按 Enter 键执行该命令。

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

以及

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

您应该可以看到类似于如下所示的输出内容：

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
            "Arn": "arn:aws:organizations::ManagementAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

编辑 Amazon Config 聚合器

您可以使用 Amazon Config 控制台或 Amazon CLI 编辑聚合器。

Editing Aggregators (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 导航到聚合器页面，然后选择聚合器名称。
3. 选择 Actions，然后选择 Edit。
4. 使用编辑聚合器页面上的相关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。

5. 选择保存。

Editing Aggregators (Amazon CLI)

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

   输入以下命令以向 **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:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

或

对于组织

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

删除 Amazon Config 聚合器

您可以使用 Amazon Config 控制台或 Amazon CLI 删除聚合器。

Deleting Aggregators (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 导航到聚合器页面，然后选择聚合器名称。
3. 选择 操作，然后选择 删除。

   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。
4. 选择 Delete 以确认您的选择。

Deleting Aggregators (Amazon CLI)

输入以下命令：

```
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。

授权聚合器账户收集 Amazon Config 配置和合规性数据

授权 是指您授予聚合器账户和区域收集 Amazon Config 配置和合规性数据的权限。如果要聚合的源账户是 Amazon Organizations 的一部分，则不需要授权。您可以使用 Amazon Config 控制台或 Amazon CLI 来授权聚合器账户。

主题

- 注意事项
- 添加授权

注意事项

聚合器有两种类型：个人账户聚合器和组织聚合器

对于个人账户聚合器，您要包含的所有源账户和区域都需要授权，包括外部账户和区域，以及组织成员账户和区域。

对于组织聚合器，组织成员账户区域不需要授权，因为授权已与 Amazon Organizations 服务集成。

聚合器不会自动代表您启用 Amazon Config

需要在源账户和区域中为任一类型的聚合器启用，Amazon Config才能在源账户和区域中生成 Amazon Config 数据。

添加授权

Adding Authorization (Console)

您可以添加授权以向聚合器账户和区域授予收集 Amazon Config 配置和合规性数据的权限。

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 导航到授权页面，然后选择添加授权。

3. 对于聚合器账户，键入聚合器账户的 12 位数账户 ID。
4. 对于聚合器区域，选择允许聚合器账户在其中收集 Amazon 配置和合规性数据的。Amazon Web Services 区域
5. 选择添加授权以确认您的选择。

   Amazon Config 会显示聚合器账户、区域和授权状态。

   > **Note**
   >
   > 您还可以使用 Amazon CloudFormation 示例模板以编程方式向聚合器账户和区域添加授权。有关更多信息，请参阅《Amazon CloudFormation 用户指南》中的 AWS::Config::AggregationAuthorization。

Authorizing a Pending Request (Console)

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

1. 选择要授权的聚合器账户，然后选择授权。

   此时会显示一条确认消息，用以确认您向聚合器账户授予从该账户收集 Amazon Config 数据的权限。
2. 再次选择授权，以确认您要向此聚合器账户授予权限。

   授权状态从请求授权更改为已授权。

授权批准期限

向个人账户聚合器添加源账户需要获得授权批准。在个人账户聚合器添加源账户后，待处理的授权批准请求将在 7 天内有效。

Adding Authorization (Amazon CLI)

1. 打开命令提示符或终端窗口。
2. 输入以下命令：

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

3. 您应该可以看到类似于如下所示的输出内容：

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

删除对聚合器账户收集 Amazon Config 配置和合规性数据的授权

授权 是指您授予聚合器账户和区域收集 Amazon Config 配置和合规性数据的权限。如果要聚合的源账户是 Amazon Organizations 的一部分，则不需要授权。您可以使用 Amazon Config 控制台或 Amazon CLI 来删除授权。

主题

- 注意事项
- 删除授权

注意事项

聚合器有两种类型：个人账户聚合器和组织聚合器

对于个人账户聚合器，您要包含的所有源账户和区域都需要授权，包括外部账户和区域，以及组织成员账户和区域。

对于组织聚合器，组织成员账户区域不需要授权，因为授权已与 Amazon Organizations 服务集成。

聚合器不会自动代表您启用 Amazon Config

需要在源账户和区域中为任一类型的聚合器启用，Amazon Config才能在源账户和区域中生成 Amazon Config 数据。

删除授权

Deleting Authorization (Console)

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 选择要删除授权的聚合器账户，然后选择删除。

   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 Amazon Config 数据。
3. 再次选择删除以确认您的选择。

   该聚合器账户现已被删除。

Deleting Authorization (Amazon CLI)

输入以下命令：

```
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。

查看 Amazon Config 聚合器

您可以使用 Amazon Config 控制台或 Amazon CLI 查看聚合器。

Viewing Aggregators (Console)

要在 Amazon Web Services 管理控制台中查看您的合规包，请参阅聚合器控制面板。

Viewing Aggregators (Amazon CLI)

1. 输入以下命令：

   ```
   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:Region:AccountID:config-aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

或

对于组织

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

Amazon Config 多账户多区域数据聚合的故障排除

Amazon 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
Amazon Config 未在组织内账户的源账户中启用。	在源账户中启用 Amazon 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 Amazon 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。

Amazon 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，Amazon Config 无法访问您的组织详细信息。	创建一个 IAM 角色，或从 IAM 角色列表中选择一个有效的 IAM 角色。 **Note** 如果 IAM 角色无效的时间超过 7 天，Amazon Config 将会删除整个组织的数据。
Amazon Config 服务访问在您的组织中处于禁用状态。	您可以通过 Amazon Config API 在 Amazon Organizations 和 `EnableAWSServiceAccess` 之间启用集成。如果您在控制台中选择添加我的组织，Amazon Config 会自动在 Amazon Config 和 Amazon Organizations 之间启用集成。
Amazon 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 控制台中启用所有功能Amazon Organizations。

如果发生这种情况	请执行该操作
中东（巴林）和亚太地区（香港）区域不会立即更新组织变更，例如添加账户、删除账户、启用服务访问权限和禁用服务访问权限。	组织变更可能会有 2 小时的延迟。请等待 2 小时以查看所有组织变更。

使用查询 Amazon 资源的当前配置状态 Amazon Config

为高级查询引入了预览功能，允许您使用生成式人工智能（生成人工智能）功能以通俗易懂的英语输入提示并将其转换为 ready-to-use查询格式。有关更多信息，请参阅适用于高级查询的自然语言查询处理器。

您可以使用 Amazon Config 根据单个账户和区域的配置属性或跨多个账户和区域查询 Amazon 资源的当前配置状态。您可以对支持的资源列表中的当前 Amazon 资源状态元数据执行基于属性的查询。Amazon Config 有关支持的资源类型列表的更多信息，请参阅支持的高级查询资源类型。

高级查询提供了单一查询终端节点和查询语言以获得当前资源状态元数据，而无需执行特定于服务的描述 API 调用。您可以使用配置聚合器从一个中央账户跨多个账户和 Amazon 地区运行相同的查询。

主题

- 功能
- Amazon Config 查询组件
- 使用适用于 Amazon Config 的 SQL 查询编辑器进行查询（控制台）
- 使用适用于 Amazon Config 的 SQL 查询编辑器进行查询（Amazon CLI）
- 用于Amazon Config高级查询的自然语言查询处理器
- Amazon Config 的示例查询
- Amazon Config 的关系查询示例
- 限制
- 高级查询的 CIDR notation/IP 范围行为
- 数组中的多个属性在高级查询中的表现
- 区域支持

功能

Amazon Config 使用结构化查询语言 (SQL) SELECT 语法的子集对当前配置项 (CI) 数据执行基于属性的查询和聚合。查询的复杂程度各不相同，从与标签 and/or 资源标识符的匹配到更复杂的查询，例如查看所有禁用版本控制的 Amazon S3 存储桶。这使您可以准确查询所需的当前资源状态，而无需执行 Amazon 特定于服务的 API 调用。

它支持聚合函数，例如、AVGCOUNT、MAX、MIN 和 SUM。

您可以使用高级查询来实现：

- 库存管理；例如，检索特定大小的亚马逊 EC2 实例列表。
- 安全和运营智能；例如，检索已启用或禁用特定配置属性的资源的列表。
- 成本优化；例如，确定未连接到任何 EC2 实例的 Amazon EBS 卷的列表。
- 合规性数据；例如，检索所有合规包及其合规性状态的列表。

有关如何使用 Amazon SQL 查询语言的信息，请参阅什么是 SQL（结构化查询语言）？ 。

Amazon Config 查询组件

Amazon Config 高级查询的 SQL SELECT 查询组件如下所示。

摘要

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

参数

[WHERE condition]

根据您指定的 condition 筛选结果。

比较运算符：、、、、、、。

- = (等于)
- IN (列出成员)
- BETWEEN (范围检查)

逻辑运算符

- AND
- OR

- NOT

[GROUP BY property]

将结果集聚合到包含与给定的属性匹配的值的行组中。

GROUP BY 子句适用于聚合。

[ORDER BY property [ASC | DESC] [, property [ASC | DESC] ...]]

按一个或多个输出 `properties` 对结果集进行排序。

当该子句包含多个属性时，结果集将根据第一个 `property` 进行排序，然后针对包含与第一个属性匹配的值的行根据第二个 `property` 进行排序，以此类推。

示例

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

使用适用于 Amazon Config 的 SQL 查询编辑器进行查询（控制台）

隆重推出适用于高级查询的预览版功能，它可让您利用生成式人工智能（生成式 AI）功能，用通俗易懂的英语输入提示，并将其转换为即用型查询格式。有关更多信息，请参阅适用于高级查询的自然语言查询处理器。

您可以使用 Amazon 示例查询，也可以创建自己的查询，称为自定义查询。

注意事项

先决条件

如果您使用的是以下 Amazon 托管式策略之一，您将拥有运行和保存查询所需的权限：AWSServiceRoleForConfig（服务相关角色）或 AWS_ConfigRole。

否则，您必须拥有 AWSConfigUserAccess Amazon 托管式策略中包含的权限。

您可以查询的属性列表

属性及其数据类型的更新列表在 GitHub 中提供。

高级查询和聚合器

要在聚合器上运行查询，请创建聚合器。有关更多信息，请参阅 为 Amazon Config 创建聚合器

如果您已经设置了聚合器，则在查询范围中，选择聚合器以在该聚合器上运行高级查询。选择聚合器时，请考虑在查询语句中添加 Amazon Web Services 账户 ID 和 Amazon 区域，以在结果中查看该信息。

使用 Amazon 示例查询

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 从左侧导航中选择 Advanced queries（高级查询），以查询针对单个账户和区域或针对多个账户和区域的资源配置。
3. 在高级查询页面上，从查询列表中选择适当的查询。您可以按名称、描述、创建者或标签在查询列表中筛选。要筛选 Amazon 查询，请选择创建者，并输入。Amazon您输入的查询将显示在 SQL 查询编辑器中。您可以根据需要编辑所选查询。
4. 要将此查询保存到新查询，请选择另存为。
   - 在查询名称字段中，更新查询的名称。
   - 在描述字段中，更新查询的描述。
   - 为此查询输入最多 50 个唯一标签。
   - 选择保存。
5. 选择运行。查询结果将显示在查询编辑器下方的表中。
6. 选择 Export as（导出为），以 CSV 或 JSON 格式导出查询结果。

创建您的自定义查询

1. 登录到，Amazon Web Services 管理控制台然后通过以下网址打开 Amazon Config 控制台：https://console.aws.amazon.com/config/home。
2. 从左侧导航中选择 Advanced queries（高级查询），以查询针对单个账户和区域或针对多个账户和区域的资源配置。

3. 要创建您的自定义查询，请选择新建查询。

   要查看或编辑自定义查询，可以按名称、描述、创建者或标签筛选查询。要筛选自定义查询，请选择创建者并输入自定义。
4. 在查询编辑器页面上，为此账户和区域创建您自己的查询。您还可以选择合适的聚合器来创建针对多个账户和区域的查询。
5. 如果您希望对此查询进行更改，请进行编辑。选择保存查询以保存此查询。

   - 在查询名称字段中，更新查询的名称。
   - 在描述字段中，更新查询的描述。
   - 为此查询输入最多 50 个唯一标签。
   - 选择保存。
6. 选择运行。查询结果将显示在查询编辑器下方的表中。
7. 选择 Export as（导出为），以 CSV 或 JSON 格式导出查询结果。

使用适用于 Amazon Config 的 SQL 查询编辑器进行查询（Amazon CLI）

Amazon CLI 是用于管理 Amazon 服务的统一工具。如果您仅使用一种工具进行下载和配置，则可通过命令行控制多个 Amazon 服务并使用脚本来自动执行这些服务。有关 Amazon CLI 的更多信息以及 Amazon CLI 工具的安装说明，请参阅《Amazon Command Line Interface 用户指南》中的以下内容。

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

如有必要，请输入 `aws configure` 以将 Amazon CLI 配置为使用一个提供高级查询的 Amazon 区域。

注意事项

先决条件

如果您使用的是以下 Amazon 托管式策略之一，您将拥有运行和保存查询所需的权限：AWSServiceRoleForConfig（服务相关角色）或 AWS_ConfigRole。

否则，您必须拥有 AWSConfigUserAccess Amazon 托管式策略中包含的权限。

您可以查询的属性列表

属性及其数据类型的更新列表在 GitHub 中提供。

高级查询和聚合器

要在聚合器上运行查询，请创建聚合器。有关更多信息，请参阅 为 Amazon Config 创建聚合器

如果您已经设置了聚合器，则在查询范围中，选择聚合器以在该聚合器上运行高级查询。选择聚合器时，请考虑在查询语句中添加 Amazon Web Services 账户 ID 和 Amazon 区域，以在结果中查看该信息。

查询资源配置数据

使用查询编辑器（Amazon CLI）查询针对单个账户和区域的资源配置数据

1. 打开命令提示符或终端窗口。
2. 输入以下命令查询您的资源配置数据。

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

根据您的查询，输出将如下所示。

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

使用查询编辑器（Amazon CLI）查询针对多个账户和区域的资源配置数据

1. 打开命令提示符或终端窗口。
2. 输入以下命令查询您的资源配置数据。

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

根据您的查询，输出将如下所示。

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> 在高级查询中使用、AWS::IAM::UserAWS::IAM::Group、AWS::IAM::Role 和 AWS::IAM::Policy 资源类型时，请使用。awsRegion = 'global'

保存查询

1. 打开命令提示符或终端窗口。
2. 输入以下命令以保存查询。

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. 根据您的查询，输出将如下所示。

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` 为可选项。传递标签时，`list-stored-queries` 或 `get-stored-query` 都不会返回保存的标签。必须使用 `list-tag-for-resources` 检索已保存查询的相关标签。
>
> 在创建或更新查询时，`--description` 是可选的。

查看所有已保存的查询

1. 输入以下命令以查看所有已保存查询的列表。

```
aws configservice list-stored-queries
```

2. 根据您的查询，输出将如下所示。

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
```

```
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

获取已保存的查询的详细信息

1. 输入以下命令以获取已保存的特定查询的详细信息。

```
aws configservice get-stored-query --query-name cli-test
```

2. 根据您的查询，输出将如下所示。

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

删除已保存的查询

- 输入以下命令以删除已保存的查询。

```
aws configservice delete-stored-query --query-name cli-test
```

如果成功，则命令会运行，而没有附加输出。

用于Amazon Config高级查询的自然语言查询处理器

> **Note**
>
> Amazon Config自然语言查询处理器的公开预览版将于 2026 年 1 月 15 日停止。此外，您还可以使用自然语言提示与 Amazon Q Developer 聊聊您的Amazon资源。有关更多信息，请参阅与 Amazon Q 开发者版聊聊您的资源。

用于高级查询的自然语言查询处理器使用 Amazon Bedrock，这是一种生成式人工智能（生成式 AI）技术，它允许您以通俗易懂的英语输入提示并将其转换为 ready-to-use查询格式。使用自然语言查询处理器，您可以对您的组织Amazon Web Services 账户或整个Amazon组织进行查询。

提示可以是问题或声明。例如，您可以输入诸如“哪些负载均衡器是在 2024 年 1 月 1 日之后创建的？”和“列出我所有运行节点 js 16 的 lambda 函数”等提示。

注意事项

自然语言查询处理器无法执行以下操作：

- 使用英语以外的语言生成查询。
- 根据与高级查询无关的提示生成查询。
- 根据超过 1000 个字符的提示生成查询。
- 根据后续更正或以前的会话生成查询。
- 解释已生成的代码。

使用自然语言查询处理器进行查询

1. 登录Amazon Web Services 管理控制台并在家中打开https://console.aws.amazon.com/config/主Amazon Config机。
2. 从左侧导航中选择 Advanced queries（高级查询），以查询针对单个账户和区域或针对多个账户和区域的资源配置。
3. 在高级查询页面上，选择新建查询，进入 查询编辑器。
   - （可选）要在聚合器上运行查询，请创建聚合器。有关更多信息，请参阅 为 Amazon Config 创建聚合器

- 如果您已经设置了聚合器，则在查询范围中，选择聚合器以在该聚合器上运行高级查询。选择聚合器时，请考虑在查询语句中添加Amazon Web Services 账户 ID 和Amazon区域，以便在结果中查看该信息。

4. 在查询编辑器中，转到自然语言查询处理器部分。用通俗易懂的英语输入提示，然后选择生成。有关示例，请参阅提示示例。
5. 您生成查询后，可以选择复制（功能上等同于 Ctrl+C）将查询复制到剪贴板，也可以选择填充到编辑器。如果已填充到编辑器中，您可以根据需要编辑生成的查询。
6. 要将此查询保存到新查询，请选择另存为。
   - 在查询名称字段中，更新查询的名称。
   - 在描述字段中，更新查询的描述。
   - 为此查询输入最多 50 个唯一标签。
   - 选择保存。
7. 选择运行。查询结果会显示在查询编辑器下方的表中。
8. 选择 Export as（导出为），以 CSV 或 JSON 格式导出查询结果。

> **Note**
>
> 查询结果将进行分页。导出时，最多可导出 500 个结果。
> 您也可以使用 APIs 来检索所有结果。结果会进行分页，您可以一次检索 100 个结果。

提示示例

以下是提示和生成查询，您可以将其用作示例。

Example: 哪些负载均衡器是在 2024 年 1 月 1 日之后创建的？

提示：What load balancers were created after January 1, 2024?

生成的查询：

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
```

```
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
    resourceCreationTime
DESC
```

Example: 可公开访问的 RDS 数据库实例都有哪些？

提示：Which of my RDS database instances are publicly accessible?

生成的查询：

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: 过去一年中创建了多少个 EC2 实例？

提示：How many EC2 instances were created in last one year?

生成的查询：

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: 我的每个 EC2 实例中有多少个Amazon Web Services 账户？

提示：How many EC2 instances do I have in each of my Amazon Web Services 账户?

生成的查询：

```
SELECT
    accountId,
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: 托管策略 AdministratorAccess 附加了哪些 IAM 角色？

提示：Which IAM roles have the managed policy AdministratorAccess attached?

生成的查询：

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: 未加密 EBS 卷

提示：EBS volumes without encryption

生成的查询：

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: 获取不合规资源

提示：Get noncompliant resources

生成的查询：

```
SELECT
    resourceId,
    resourceType
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: 列出我所有运行节点 js 16 的 lambda 函数

提示：List all my lambda function that is running node js 16

生成的查询：

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: 哪些 ACM 证书将在接下来的 30 天内过期？

提示：What ACM certificates expire the next 30 days?

生成的查询：

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53'
```

> **Note**
>
> 生成的查询中的时间取决于您输入提示的时间。

提供反馈

您可以提供有关自然语言查询处理器的总体反馈或有关生成的特定查询的反馈。

提供有关自然语言查询处理器的反馈

选择右侧自然语言查询处理器上方显示的提供反馈按钮。您可以输入您的满意度或不满意度，并提供有关Amazon Config如何使自然语言查询更有用的反馈。

> **Note**
>
> 请勿透露任何个人、商业敏感或机密信息。

就生成的特定查询提供反馈

您可以通过选择生成的查询下方的大拇指向上或大拇指向下按钮来提供有关生成的查询的反馈。

区域支持

自然语言查询处理器在以下区域受支持。

区域名称	区域	端点	协议
美国东部(弗吉尼亚北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS

Amazon Config 的示例查询

查看以下示例查询。

Query to list all EC2 instances with AMI ID ami-12345

查询：

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

结果：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
            {
                "Name": "availabilityZone"
            }
```

```
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\"resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their Amazon Config rules compliance status

查询：

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

结果：

```
{
    "QueryInfo": {
```

```
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of Amazon Conformance packs

查询：

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

结果：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
            },
            {
```

```
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of Amazon resources grouped by account ID

查询：

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

结果：

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
}
```

Query to list all EC2 volumes that are not in use

查询：

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

结果：

```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
    ],
    "QueryInfo": {
```

```
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

Amazon Config 的关系查询示例

查看以下关系查询示例。

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

或

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
```

```
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

限制

> **Note**
>
> 高级查询不支持查询尚未配置为由配置记录器记录的资源。 Amazon Config 当发现资源但未配置为由配置记录器记录`configurationItemStatus`时，将在`ResourceNotRecorded`中创建配置项目 (CIs)。虽然聚合器会聚合这些数据 CIs，但高级查询不支持 CIs 使用进行`ResourceNotRecorded`查询。更新您的记录器设置以启用记录要查询的资源类型。

作为 SQL `SELECT` 的一个子集，查询语法有以下限制：

- 查询中不支持、`ALLAS`、`DISTINCT`、`FROM`、`HAVING`、`JOIN` 和 `UNION` 关键字。不支持 `NULL` 值查询。

- 不支持在查询中使用复杂 CASE 语句来直接创建优先级字段。
- 不支持查询第三方资源。使用高级查询检索的第三方资源的配置字段将设置为。NULL
- 不支持使用 SQL 查询解包嵌套结构（例如标签）。
- 不支持查询已删除资源。要发现已删除的资源，请参阅查找发现的资源 Amazon Config。
- 针对所有列的 SELECT 简写形式（也就是 SELECT *）将仅选择 CI 的顶级标量属性。返回的标量属性
  为、accountIdawsRegion、arn、availabilityZone、configurationItemCaptureTime、resc
  和 version。
- 通配符限制：
  - 通配符仅支持属性值，但不支持属性键（例如支持，...WHERE someKey LIKE 'someValue%'但不支持 ...WHERE 'someKey%' LIKE 'someValue%'）。
  - 仅支持后缀通配符（例如，支持 ...LIKE 'AWS::EC2::%' 和，...LIKE 'AWS::EC2::_'但不支持 ...LIKE '%::EC2::Instance' 和 ...LIKE '_::EC2::Instance'）。
  - 通配符匹配项的长度必须至少为 3 个字符（例如，不允许 ...LIKE 'ab%' 和，...LIKE 'ab_'但允许 ...LIKE 'abc%' 和 ...LIKE 'abc_'）。

  > **Note**
  >
  > “_”（单下划线）也被视为通配符。

- 聚合限制：
  - 聚合函数仅可接受一个参数或属性。
  - 聚合函数无法采用其他函数作为参数。
  - 带有引用聚合函数的 ORDER BY 子句的 GROUP BY 只能包含一个属性。
  - 对于所有其他聚合，GROUP BY 子句最多可以包含三个属性。
  - 除 ORDER BY 子句具有聚合函数外，所有聚合查询都支持分页。例如，如果 Y 是聚合函数，则 GROUP BY X, ORDER BY Y 不起作用。
  - 不支持聚合中的 HAVING 子句。
- 不匹配的标识符限制：

  不匹配的标识符是拼写相同但大小写不同（大写和小写）的属性。高级查询不支持处理包含不匹配标识符的查询。例如：
  - 两个拼写完全相同但大小写不同的属性（configuration.dbclusterIdentifier 和 configuration.dBClusterIdentifier）。

- 两个属性，其中一个属性是另一个属性的子集，并且它们的大小写不同（configuration.ipAddress 和 configuration.ipaddressPermissions）。

高级查询的 CIDR notation/IP 范围行为

CIDR 表示法将转换为 IP 范围以供搜索。

这意味着，"=" 和 "BETWEEN" 会搜索任何包含所提供的 IP 的范围，而不是精确的范围。

要搜索精确的 IP 范围，您需要添加其他条件以排除在范围 IPs 之外。

Example 搜索确切的 CIDR 块 10.0.0.0/24

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

Example 搜索确切的 IP 地址 192.168.0.2/32

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

数组中的多个属性在高级查询中的表现

当针对对象数组内的多个属性执行查询时，将针对所有数组元素计算匹配项。

例如，对于具有规则 A 和 B 的资源 R，该资源符合规则 A 但不符合规则 B。资源 R 存储为：

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
```

```
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

此查询将返回 R：

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

第一个条件`configuration.configRuleList.complianceType = 'non_compliant'`适用于 R 中的所有元素configRuleList，因为 R 有一条 complianceType = 'non_complitive' 的规则（规则 B），因此该条件被评估为真。

第二个条件适用`configuration.configRuleList.configRuleName`于 R 中的所有元素 configRuleList，因为 R 的规则（规则 A）为 configRuleName = 'A'，因此该条件被评估为真。由于两个条件均为 True，因此将返回 R。

区域支持

以下区域支持高级查询：

区域名称	区域	端点	协议	
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
美国西部（北加利福尼亚）	us-west-1	config.us-west-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议	
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS	
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS	
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
亚太地区（马来西亚）	ap-southeast-5	config.ap-southeast-5.amazonaws.com	HTTPS	
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
亚太地区（新西兰）	ap-southeast-6	config.ap-southeast-6.amazonaws.com	HTTPS	
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS	

区域名称	区域	端点	协议
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（台北）	ap-east-2	config.ap-east-2.amazonaws.com	HTTPS
亚太地区（泰国）	ap-southeast-7	config.ap-southeast-7.amazonaws.com	HTTPS
亚太地区（东京）	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
中国（北京）	cn-north-1	config.cn-north-1.amazonaws.com.cn	HTTPS
中国（宁夏）	cn-northwest-1	config.cn-northwest-1.amazonaws.com.cn	HTTPS

区域名称	区域	端点	协议	
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS	
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS	
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS	
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS	
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS	
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS	
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS	
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS	
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS	
墨西哥（中部）	mx-central-1	config.mx-central-1.amazonaws.com	HTTPS	
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS	

区域名称	区域	端点	协议	
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS	
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS	

删除 Amazon Config 数据

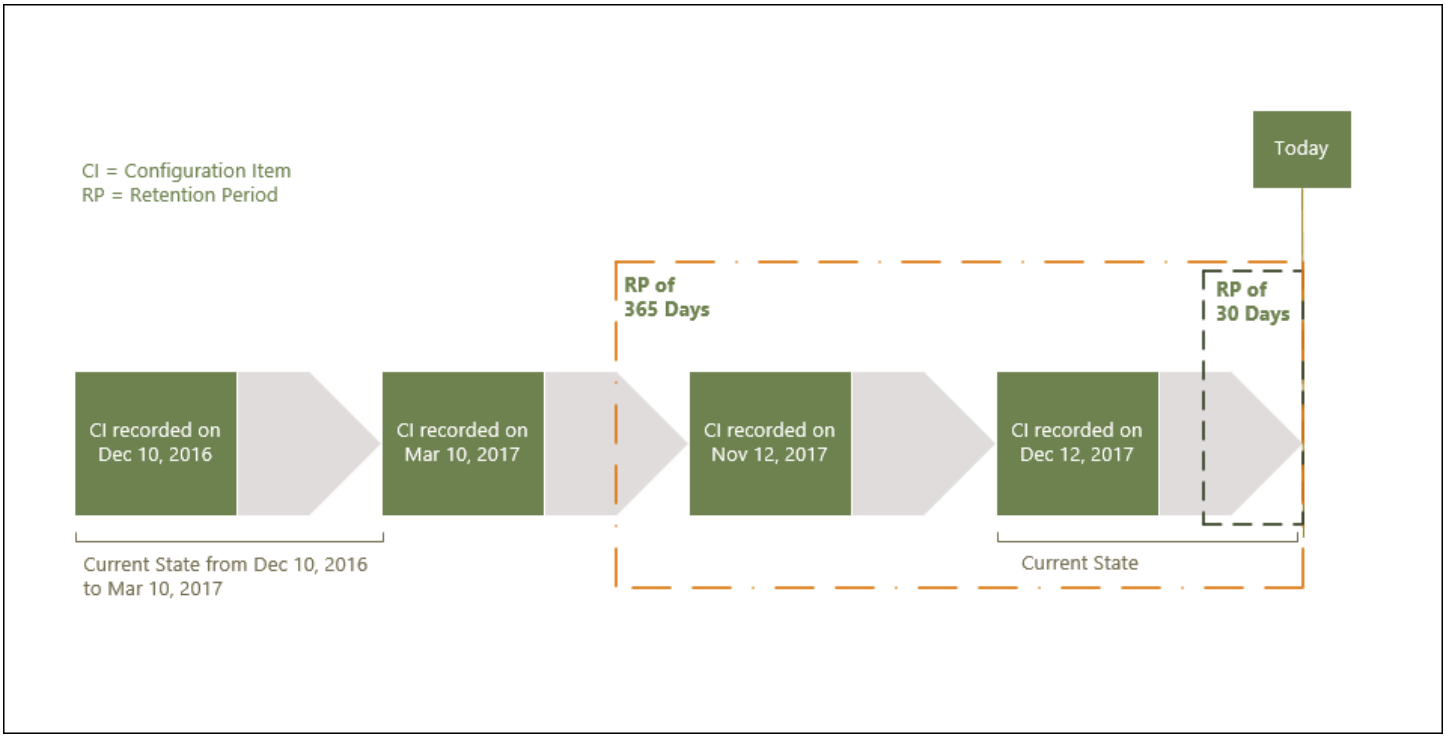
> **Note**
>
> 虽然 Amazon Config 使用 Amazon Simple Storage Service（Amazon S3）和 Amazon Simple Notification Service（Amazon SNS）发送配置快照和配置历史记录文件，但 Amazon Config 拥有自己的数据存储和保留策略。此页面上的信息专门针对。Amazon ConfigAmazon S3 和 Amazon SNS 有各自独立的数据存储和保留策略。

Amazon Config 允许您通过为 `ConfigurationItems` 指定保留期来删除您的数据。指定保留期后，Amazon Config 会将您的 `ConfigurationItems` 保留指定的时间段。您可以选择介于最少 30 天和最多 7 年（2557 天）之间的保留期。Amazon Config 会删除超过您指定的保留期的数据。如果您未指定保留期，Amazon Config 将继续在默认保留期 7 年（2557 天）内存储。`ConfigurationItems`当记录功能打开时，资源的当前状态是 `ConfigurationItem` 被记录，直到记录下一个更改（新的 `ConfigurationItem`）。

为了理解保留期的行为，我们来看一下时间表。

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

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



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

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

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

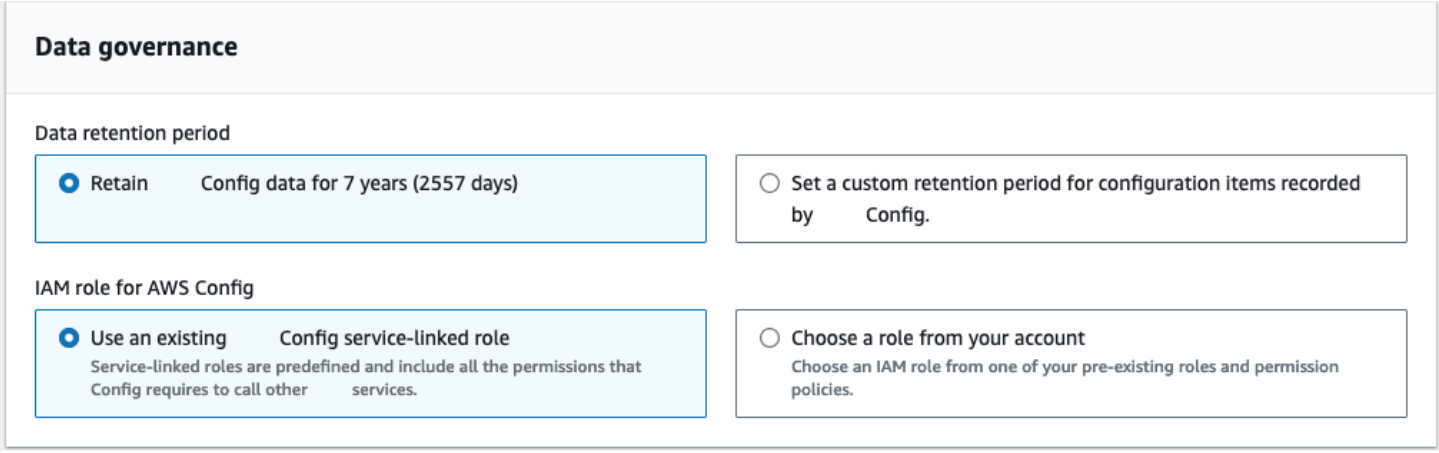
> **Note**
>
> - 如果记录功能已关闭，则 Amazon Config 无法记录您的。`ConfigurationItems`
> - 如果您的 IAM 角色权限不足，Amazon Config 将无法记录您的。`ConfigurationItems`有关更多信息，请参阅分配给 Amazon Config 的 IAM 角色的权限。

在 Amazon Web Services 管理控制台 中设置数据保留期

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

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

下图显示了您可以在数据治理中设置数据留存期限的位置。您可以从 Amazon Config 控制台访问编辑设置页面上的数据治理，方法是选择左侧导航栏中的设置，然后选择编辑。



安全性 Amazon Config

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

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

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

本文档可帮助您了解在使用时如何应用分担责任模型 Amazon Config。以下主题向您介绍如何进行配置 Amazon Config 以满足您的安全和合规性目标。

主题

- 中的数据保护 Amazon Config
- Identity and Access Management Amazon Config
- 中的事件响应 Amazon Config
- 的合规性验证 Amazon Config
- 韧性在 Amazon Config
- 中的基础设施安全 Amazon Config
- 防止跨服务混淆代理
- 的安全最佳实践 Amazon Config

中的数据保护 Amazon Config

分担责任模型适用于 Amazon Config 中的数据保护。如本模型所述 Amazon ，负责保护运行所有内容的全球基础架构 Amazon Web Services 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

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

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

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

静态数据加密

使用透明的服务器端加密，加密静态数据。这样可以帮助减少在保护敏感数据时涉及的操作负担和复杂性。通过静态加密，您可以构建符合加密合规性和法规要求的安全敏感型应用程序。

传输中的数据的加密

收集和访问的数据只能通过 Amazon Config 受传输层安全 (TLS) 保护的通道进行。

Identity and Access Management Amazon Config

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

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 如何 Amazon Config 与 IAM 配合使用
- 基于身份的策略示例 Amazon Config
- Amazon 的托管策略 Amazon Config
- 分配给的 IAM 角色的权限 Amazon Config
- 更新客户管理的配置记录器的 IAM 角色
- Amazon Config 传送渠道的 Amazon S3 存储桶的权限
- Amazon Config 交付渠道 KMS 密钥的权限
- Amazon SNS 主题的权限
- 对 Amazon Config 身份和访问进行故障排除
- 将服务相关角色用于 Amazon Config

受众

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

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅对 Amazon Config 身份和访问进行故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅如何 Amazon Config 与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅基于身份的策略示例 Amazon Config）

使用身份进行身份验证

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

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

Amazon Web Services 账户 root 用户

创建时 Amazon Web Services 账户，首先会有一个名为 Amazon Web Services 账户 root 用户的登录身份，该身份可以完全访问所有资源 Amazon Web Services 服务 和资源。我们强烈建议不要使用根

用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

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

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

IAM 用户和群组

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

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

IAM 角色

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

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

使用策略管理访问

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

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

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

基于身份的策略

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

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

基于资源的策略

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

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

其他策略类型

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

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

多个策略类型

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

如何 Amazon Config 与 IAM 配合使用

在使用 IAM 管理访问权限之前 Amazon Config，请先了解哪些可用的 IAM 功能 Amazon Config。

您可以搭配使用的 IAM 功能 Amazon Config

IAM 功能	Amazon Config 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACLs	否
ABAC（策略中的标签）	是
临时凭证	是
转发访问会话（FAS）	是
服务角色	是
服务关联角色	是

要全面了解 Amazon Config 以及其他 Amazon 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的Amazon 服务。

基于身份的策略 Amazon Config

支持基于身份的策略：是

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

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

基于身份的策略示例 Amazon Config

要查看 Amazon Config 基于身份的策略的示例，请参阅。基于身份的策略示例 Amazon Config

内部基于资源的政策 Amazon Config

支持基于资源的策略：否

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

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

的政策行动 Amazon Config

支持策略操作：是

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

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

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

正在执行的策略操作在操作前 Amazon Config 使用以下前缀：

```
config
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 Describe 开头的所有操作，包括以下操作：

```
"Action": "config:Describe*"
```

要查看 Amazon Config 基于身份的策略的示例，请参阅。基于身份的策略示例 Amazon Config

的政策资源 Amazon Config

支持策略资源：是

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

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

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

要查看 Amazon Config 资源类型及其列表 ARNs，请参阅《服务授权参考》 Amazon Config中定义的资源。要了解可以在哪些操作中指定每个资源的 ARN，请参阅 Amazon Config定义的操作。

要查看 Amazon Config 基于身份的策略的示例，请参阅。基于身份的策略示例 Amazon Config

的策略条件密钥 Amazon Config

支持特定于服务的策略条件键：是

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

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

要查看 Amazon Config 条件键列表，请参阅《服务授权参考》 Amazon Config中的条件密钥。要了解可以使用条件键的操作和资源，请参阅由定义的操作 Amazon Config。

要查看 Amazon Config 基于身份的策略的示例，请参阅。基于身份的策略示例 Amazon Config

ACLs in Amazon Config

支持 ACLs：否

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

ABAC with Amazon Config

支持 ABAC（策略中的标签）：是

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

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

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

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

有关为 Amazon Config 资源添加标签的更多信息，请参阅标记您的 Amazon Config 资源。

将临时凭证与配合使用 Amazon Config

支持临时凭证：是

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

转发访问会话 Amazon Config

支持转发访问会话（FAS）：是

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

Amazon Config的服务角色

支持服务角色：是

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

> **Warning**
>
> 更改服务角色的权限可能会破坏 Amazon Config 的功能。只有在 Amazon Config 提供操作指导时才编辑服务角色。

的服务相关角色 Amazon Config

支持服务关联角色：是

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

有关创建或管理 Amazon Config 服务相关角色的详细信息，请参阅将服务相关角色用于 Amazon Config。

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

基于身份的策略示例 Amazon Config

默认情况下，用户和角色没有创建或修改 Amazon Config 资源的权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

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

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

主题

- 策略最佳实践
- 注册获取 Amazon Web Services 账户
- 保护 IAM 用户
- 使用 Amazon Config 控制台
- 允许用户查看他们自己的权限
- 只读访问权限 Amazon Config
- 完全访问权限 Amazon Config
- Amazon Config 规则 API 操作支持的资源级权限
- 支持多账户多区域数据聚合的资源级别权限

策略最佳实践

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

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

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

注册获取 Amazon Web Services 账户

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

报名参加 Amazon Web Services 账户

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

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

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

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

保护 IAM 用户

注册后 Amazon Web Services 账户，开启多重身份验证 (MFA)，保护您的管理用户。有关说明，请参阅《IAM 用户指南》中的 为 IAM 用户启用虚拟 MFA 设备（控制台）。

要允许其他用户访问您的 Amazon Web Services 账户 资源，请创建 IAM 用户。为了保护您的 IAM 用户，请启用 MFA 并仅向 IAM 用户授予执行任务所需的权限。

有关创建和保护 IAM 用户的更多信息，请参阅《IAM 用户指南》中的以下主题：

- 在你的 IAM 用户中创建 Amazon Web Services 账户
- 适用于 Amazon 资源的访问权限管理
- 基于 IAM 身份的策略示例

使用 Amazon Config 控制台

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

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

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

您必须向用户授予与之交互的权限 Amazon Config。对于需要完全访问托管权限的用户 Amazon Config，请使用对 Amazon Config托管的完全访问权限策略。

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

允许用户查看他们自己的权限

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

只读访问权限 Amazon Config

以下示例显示了一个 Amazon 托管策略，AWSConfigUserAccess该策略授予对的只读访问权限 Amazon Config。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

在这些策略语句中，Effect 元素指定是允许还是拒绝操作。Action 元素列出了允许用户执行的特定操作。Resource元素列出了允许用户对其执行这些操作的 Amazon 资源。对于控制 Amazon Config 操作访问权限的策略，Resource元素始终设置为 *，通配符表示 “所有资源”。

Action元素中的值对应 APIs 于服务支持的值。动作前面有表示它们指的是 Amazon Config 动作。config:您可以在 * 元素中使用 Action 通配符，如以下示例所示：

- "Action": ["config:*ConfigurationRecorder"]

  这允许所有以 “ConfigurationRecorder”（StartConfigurationRecorder，StopConfigurationRecorder）结尾的 Amazon Config 操作。

- "Action": ["config:*"]

  这允许所有 Amazon Config 操作，但不允许对其他 Amazon 服务执行操作。

- "Action": ["*"]

  这允许所有 Amazon 操作。此权限适用于担任您账户 Amazon 管理员的用户。

只读策略不对用户授予执行、StartConfigurationRecorderStopConfigurationRecorder 和 DeleteConfigurationRecorder 操作的权限。不允许使用此策略的用户启动配置记录器、停止配置记录器或删除配置记录器。有关 Amazon Config 操作列表，请参阅 Amazon Config API 参考。

完全访问权限 Amazon Config

以下示例显示了授予对的完全访问权限的策略 Amazon Config。它授予用户执行所有 Amazon Config 操作的权限。它还允许用户管理 Amazon S3 存储桶中的文件，以及管理与用户关联的账户中的 Amazon SNS 主题。

> **Important**
>
> 此策略授予广泛的权限。在授予完全访问权限之前，请考虑从最低权限集开始，并根据需要授予其他权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说是更好的做法。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

Amazon Config 规则 API 操作支持的资源级权限

资源级权限是指能够指定允许用户对哪些资源执行操作。 Amazon Config 支持某些 Amazon Config 规则 API 操作的资源级权限。这意味着，对于某些 Amazon Config 规则操作，您可以控制何时允许用户使用这些操作的条件。这些条件可以是必须满足的操作，也可以是允许用户使用的特定资源。

下表描述了当前支持资源级权限的 Amazon Config 规则 API 操作。它还描述了每个操作支持的资源及其 ARNs对应的资源。指定 ARN 时，可以在路径中使用* 通配符；例如，当您无法或不想指定确切的资源时。 IDs

> **Important**
>
> 如果此表中未列出 Amazon Config 规则 API 操作，则该操作不支持资源级权限。如果 Amazon Config 规则操作不支持资源级权限，则可以向用户授予使用该操作的权限，但必须为策略语句的资源元素指定*。

API 操作	资源
DeleteConfigRule	Config 规则 arn: aws: config:: config-rule/config-rule *region:accountID ID*
DeleteEvaluationResults	Config 规则 arn: aws: config:: config-rule/config-rule *region:accountID ID*
DescribeCompliance ByConfigRule	Config 规则 arn: aws: config:: config-rule/config-rule *region:accountID ID*
DescribeConfigRuleEvaluatio nStatus	Config 规则 arn: aws: config:: config-rule/config-rule *region:accountID ID*
GetComplianceDetailsByConfi gRule	Config 规则 arn: aws: config:: config-rule/config-rule *region:accountID ID*
PutConfigRule	Config 规则 arn: aws: config:: config-rule/config-rule *region:accountID ID*
StartConfigRulesEvaluation	Config 规则 arn: aws: config:: config-rule/config-rule *region:accountID ID*
PutRemediationConfigurations	修复配置

API 操作	资源
	arn: aws: config:: 修正配置/*region:accountId config rule name/remediation configuration id*
DescribeRemediationConfigurations	修复配置 arn: aws: config:: 修正配置/*region:accountId config rule name/remediation configuration id*
DeleteRemediationConfiguration	修复配置 arn: aws: config:: 修正配置/*region:accountId config rule name/remediation configuration id*
PutRemediationExceptions	修复配置 arn: aws: config:: 修正配置/*region:accountId config rule name/remediation configuration id*
DescribeRemediationExceptions	修复配置 arn: aws: config:: 修正配置/*region:accountId config rule name/remediation configuration id*
DeleteRemediationExceptions	修复配置 arn: aws: config:: 修正配置/*region:accountId config rule name/remediation configuration id*

例如，您希望允许特定用户对特定规则进行的读访问，但拒绝特定用户对特定规则进行的写访问。

在第一个策略中，您可以允许 Amazon Config 规则读取操作，例如`DescribeConfigRuleEvaluationStatus`对指定规则的读取操作。

JSON

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

```
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "config:StartConfigRulesEvaluation",
                "config:DescribeComplianceByConfigRule",
                "config:DescribeConfigRuleEvaluationStatus",
                "config:GetComplianceDetailsByConfigRule"
            ],
            "Resource": [
                "arn:aws:config:us-east-1:123456789012:config-rule/config-
rule-ID",
                "arn:aws:config:us-east-1:123456789012:config-rule/config-
rule-ID"
            ]
        }
    ]
}
```

在第二个策略中，您拒绝对特定 Amazon Config 规则执行规则写入操作。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
            ],
            "Resource": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-ID"
        }
    ]
}
```

使用资源级权限，您可以允许读取权限和拒绝写入权限，以便对 Amazon Config 规则 API 操作执行特定操作。

支持多账户多区域数据聚合的资源级别权限

您可以使用资源级权限控制用户对多账户多区域数据聚合执行特定操作的能力。以下 Amazon Config `Aggregator` APIs 支持资源级别权限：

- BatchGetAggregateResourceConfig
- DeleteConfigurationAggregator
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSourcesStatus
- GetAggregateComplianceDetailsByConfigRule
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResourceCounts
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfigurationAggregator
- SelectAggregateResourceConfig

例如，您可以通过创建两个聚合器 `AccessibleAggregator` 和，`InAccessibleAggregator`并附加允许访问 `AccessibleAggregator` 但拒绝访问 `InAccessibleAggregator` 的 IAM 策略来限制特定用户对资源数据的访问。

适用于 IAM 的政策 AccessibleAggregator

在此策略中，您允许访问您指定的 Amazon Config Amazon 资源名称（ARN）支持的聚合器操作。在此示例中， Amazon Config ARN 是。`arn:aws:config:ap-northeast-1:`*`AccountID`*`:config-aggregator/config-aggregator-mocpsqhs`

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-mocpsqhs"
        }
    ]
}
```

适用于 IAM 的政策 InAccessibleAggregator

在此策略中，您允许访问您指定的 Amazon Config ARN 支持的聚合器操作。在此示例中， Amazon Config ARN 是。`arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
```

```
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
}
```

如果开发者组的用户尝试对您指定的 Amazon Config ARN 执行任何此类操作，该用户将收到拒绝访问异常。

检查用户访问权限

要显示您创建的聚合器，请运行以下 Amazon CLI 命令：

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

命令成功完成后，您将能够看到与您的账户关联的所有聚合器的详细信息。在此示例中，这些聚合器是 AccessibleAggregator 和 InAccessibleAggregator：

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
```

```
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> account-aggregation-sources输入要为其汇总数据的 Amazon 帐户 IDs 的逗号分隔列表。将账户 IDs 用方括号括起来，并确保对引号进行转义（例如，"[{\"AccountIds\": [\"*AccountID1*\",\"*AccountID2*\",\"*AccountID3*\"],\"AllAwsRegions\": true}]"）。

附加以下 IAM 策略以拒绝访问 InAccessibleAggregator 或您要拒绝访问的聚合器。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:111122223333:config-
aggregator/config-aggregator-pokxzldx"
        }
    ]
}
```

接下来，您可以确认 IAM 策略是否适用于限制对特定聚合器规则的访问：

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

此命令应返回拒绝访问异常：

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
```

```
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

Amazon 的托管策略 Amazon Config

Amazon 托管策略是由创建和管理的独立策略 Amazon。 Amazon 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， Amazon 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新 Amazon 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 Amazon 最有可能在启动新的 API 或现有服务可以使用新 Amazon Web Services 服务 的 API 操作时更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

Amazon 托管策略：AWSConfigServiceRolePolicy

Amazon Config 使用名AWSServiceRoleForConfig为的服务关联角色代表您呼叫其他 Amazon 服务。使用 Amazon Web Services 管理控制台 进行设置时 Amazon Config， Amazon Config 如果您选择使用 SLR 而不是您自己的 Amazon Identity and Access Management (IAM) 服务角色，则会自动创建此 Amazon Config SLR。

AWSServiceRoleForConfig SLR 包含托管策略。`AWSConfigServiceRolePolicy`此托管策略包含 Amazon Config 资源的只读和只写权限，以及其他支持的服务中资源的只读权限。 Amazon Config 该策略提供全面的访问权限，用于监控和记录整个 Amazon 基础架构的配置更改，包括计算、存储、联网、安全、分析和机器学习服务等 100 Amazon 多种服务的权限。

该策略包括以下服务类别的权限：

- `access-analyzer`— 允许委托人分析访问模式并检索安全发现。
- `account`— 允许委托人检索账户联系信息。
- `acm`和 `acm-pca` — 允许委托人管理 SSL/TLS 证书和私有证书颁发机构。
- `airflow`— 允许委托人监视托管的 Apache Airflow 环境。
- `amplify`和 `amplifyuibuilder` — 允许委托人监视 Web 应用程序和用户界面组件。
- `aoss`— 允许委托人监控 OpenSearch 无服务器集合和安全配置。

- app-integrations— 允许委托人监视应用程序集成配置。
- appconfig— 允许委托人监视应用程序配置部署。
- appflow— 允许委托人监视应用程序之间的数据流配置。
- application-autoscaling和 application-signals — 允许委托人监控自动缩放策略和应用程序性能指标。
- appmesh— 允许委托人监视服务网格配置。
- apprunner— 允许委托人监控容器化的 Web 应用程序和服务。
- appstream— 允许委托人监视应用程序流配置。
- appsync— 允许委托人监控 GraphQL API 配置。
- aps— 允许委托人监视 Prometheus 的监控配置。
- apptest— 允许校长监视应用程序测试配置。
- arc-zonal-shift— 允许校长监控分区班配置的可用性。
- athena— 允许委托人监视查询引擎配置和数据目录。
- auditmanager— 允许校长监控审计和合规性评估。
- autoscaling和 autoscaling-plans — 允许委托人监控自动缩放组和扩展计划。
- b2bi— 允许委托人监视 business-to-business集成配置。
- backup和 backup-gateway — 允许委托人监视备份策略和网关配置。
- batch— 允许委托人监视批处理计算环境和作业队列。
- bcm-data-exports— 允许委托人监控账单和成本管理数据的导出。
- bedrock和 bedrock-agentcore — 允许委托人监控基础模型和 AI 代理配置。
- billingconductor— 允许委托人监控账单组配置。
- budgets— 允许委托人监控预算配置和操作。
- cassandra— 允许委托人查询托管 Cassandra 数据库配置。
- ce— 允许委托人监控成本和使用情况报告配置。
- cleanrooms和 cleanrooms-ml — 允许校长监控数据协作和机器学习配置。
- cloud9— 允许委托人监控云开发环境配置。
- cloudformation— 允许委托人将基础架构作为代码堆栈配置进行监视。
- cloudfront— 允许委托人监控内容分发网络配置。
- cloudtrail— 允许委托人监控 API 日志记录和审计跟踪配置。
- cloudwatch— 允许委托人监控指标、警报和仪表板配置。

- codeartifact— 允许委托人监视软件包存储库配置。
- codebuild— 允许委托人监视生成项目配置。
- codecommit— 允许委托人监视源代码存储库的配置。
- codeconnections— 允许委托人监视第三方源连接。
- codedeploy— 允许委托人监视应用程序部署配置。
- codeguru-profiler和 codeguru-reviewer — 允许委托人监视代码分析和性能分析配置。
- codepipeline— 允许委托人监控持续集成和部署管道配置。
- codestar-connections— 允许委托人监视开发者工具的连接。
- cognito-identity和 cognito-idp — 允许委托人监控身份和用户池配置。
- comprehend— 允许委托人监视自然语言处理配置。
- config— 允许委托人管理配置记录和合规性监控。
- connect— 允许校长监控联络中心配置。

有关支持的资源类型的更多信息，请参阅支持的资源类型 Amazon Config和将服务相关角色用于 Amazon Config。

要查看有关策略（包括 JSON 策略文档的最新版本）的更多信息，请参阅《Amazon 托管式策略参考指南》中的 AWSConfigServiceRolePolicy。

> **推荐：使用服务相关角色**
>
> 除非您有特定的使用案例，否则建议您使用服务相关角色。服务相关角色可添加 Amazon Config 按预期运行所需的所有必要权限。某些功能（例如服务相关配置记录器）要求您使用服务相关角色。

Amazon 托管策略：AWS_ConfigRole

要记录您的 Amazon 资源配置， Amazon Config 需要 IAM 权限才能获取有关您的资源的配置详细信息。如果要为 Amazon Config创建 IAM 角色，可以使用管理型策略 AWS_ConfigRole 并将其附加到 IAM 角色。

每次 Amazon Config 添加对 Amazon 资源类型的支持时，此 IAM 策略都会更新。这意味着，只要 AWS_ConfiGrole 角色附加了此托管策略，它 Amazon Config 将继续拥有记录所支持资源类型的配置数据所需的权限。该策略提供全面的访问权限，用于监控和记录整个 Amazon 基础架构的配置更改，

包括计算、存储、联网、安全、分析和机器学习服务等 100 Amazon 多种服务的权限。有关更多信息，请参阅支持的资源类型 Amazon Config和分配给的 IAM 角色的权限 Amazon Config。

要查看有关该策略的更多详细信息，包括最新版本的 JSON 策略文档，请参阅《Amazon 托管策略参考指南》中的 AWS_ConfiGrole。

Amazon 托管策略：AWSConfigUserAccess

此 IAM 政策提供使用权限 Amazon Config，包括按资源标签搜索和读取所有标签。这不提供配置权限 Amazon Config，而配置权限需要管理权限。

查看策略：AWSConfigUserAccess。

Amazon 托管策略：ConfigConformsServiceRolePolicy

要部署和管理一致性包， Amazon Config 需要 IAM 权限和其他 Amazon 服务的特定权限。它们允许您部署和管理具有完整功能的一致性包，并且每次都会更新，为一致性包 Amazon Config 添加新功能。有关合规包的更多信息，请参阅合规包。

查看策略：ConfigConformsServiceRolePolicy。

Amazon 托管策略：AWSConfigRulesExecutionRole

要部署 Amazon 自定义 Lambda 规则， Amazon Config 需要 IAM 权限和其他 Amazon 服务的特定权限。它们允许 Amazon Lambda 函数访问定期发送到 Amazon S3 的 Amazon Config Amazon Config API 和配置快照。评估 Amazon 自定义 Lambda 规则的配置更改的函数需要此访问权限，并且每次 Amazon Config 添加新功能时都会更新。有关 Amazon 自定义 Lambda 规则的更多信息，请参阅创建自定义 Amazon Config Lambda 规则。有关配置快照的更多信息，请参阅概念 | 配置快照。有关传输配置快照的更多信息，请参阅管理传输通道。

查看策略：AWSConfigRulesExecutionRole。

Amazon 托管策略：AWSConfigMultiAccountSetupPolicy

要在组织中的成员账户中集中部署、更新和删除 Amazon Config 规则和合规包 Amazon Organizations， Amazon Config 需要 IAM 权限和其他 Amazon 服务的特定权限。每次 Amazon Config 为多账户设置添加新功能时，都会更新此托管策略。有关更多信息，请参阅管理组织中所有账户的 Amazon Config 规则和管理组织中所有账户的合规包。

查看策略：AWSConfigMultiAccountSetupPolicy。

Amazon 托管策略：AWSConfigRoleForOrganizations

Amazon Config 要允许只读调用 Amazon Organizations APIs， Amazon Config 需要 IAM 权限和其他 Amazon 服务的特定权限。每次 Amazon Config 为多账户设置添加新功能时，都会更新此托管策略。有关更多信息，请参阅管理组织中所有账户的 Amazon Config 规则和管理组织中所有账户的合规包。

查看策略：AWSConfigRoleForOrganizations。

Amazon 托管式策略：AWSConfigRemediationServiceRolePolicy

Amazon Config 要允许代表您修复NON_COMPLIANT资源， Amazon Config 需要 IAM 权限和其他 Amazon 服务的特定权限。每次 Amazon Config 添加新的补救功能时，都会更新此托管策略。有关修复的更多信息，请参阅使用规则修复不合规的 Amazon Config 资源。有关启动可能的 Amazon Config 评估结果的条件的更多信息，请参阅概念 | Amazon Config 规则。

查看策略：AWSConfigRemediationServiceRolePolicy。

Amazon ConfigAmazon 托管策略的更新

查看 Amazon Config 自该服务开始跟踪这些更改以来 Amazon 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 “ Amazon Config 文档历史记录” 页面上的 RSS feed。

更改	描述	日期
AWS_ConfigRole— 添加 “s3tables：ListTagsForResource”、“s3tables：”、“s3tables：GetTableBucketMetricsConfiguration” GetTableBucketStorageClass	此策略现在支持 S3Tables 的额外权限。	2026年1月9日
AWSConfigServiceRolePolicy— 添加 “s3tables：ListTagsForResource”、“s3tables：”、“s3tables：GetTableBucketMetricsConfiguration” GetTableBucketStorageClass	此策略现在支持 S3Tables 的额外权限。	2026年1月9日

更改	描述	日期
AWS_ConfigRole— 添加 “lightsail:GetActiveNames” “lightsail:GetOperations” “s3:” GetBucketAbac	该政策现在支持亚马逊 Lightsail 和亚马逊简单存储服务 (Amazon S3) 的额外权限。	2025 年 11 月 20 日
AWSConfigServiceRolePolicy— 添加 “lightsail:GetActiveNames” “lightsail:GetOperations” “s3:” GetBucketAbac	该政策现在支持亚马逊 Lightsail 和亚马逊简单存储服务 (Amazon S3) 的额外权限。	2025 年 11 月 20 日
AWSConfigServiceRolePolicy— 更新了托管策略，具有在 100 多种 Amazon 服务（包括计算、存储、联网、安全、分析和机器学习服务）中记录 Amazon 资源配置的全面权限。	现在，该策略提供了有关服务权限的增强文档，并支持对所有 Amazon Config 支持配置记录的 Amazon 服务进行全面监控。	2025 年 11 月 11 日
AWS_ConfigRole— 更新了托管策略，具有跨多种服务记录 Amazon 资源配置的全面权限 Amazon Identity and Access Management，包括亚马逊弹性计算云、亚马逊简单存储服务 Amazon Lambda、Amazon Relational Database Service 等。	此策略现在支持额外权限，以便在所有支持的 Amazon 服务中进行全面的 Amazon 资源配置记录和监控。	2025 年 11 月 10 日

更改	描述	日期
AWS_ConfigRole— 添加“放大：” “放大：GetDomainAssociation” “放大：” “appsync：ListDomainAssociations” “appsync：ListTagsForResource” “bedrock：GetSourceApiAssociation” “bedrock：ListSourceApiAssociations” “bedrock：GetFlow” “bedrock：ListAgentCollaborators” “cloudFormation：ListFlows” “codeartifact：ListPrompts” “codeartifact：GetResourcePolicy” “codeartifact：DescribePublisherDescribePackageGroup” “codepipeline：ListAllowedRepositoriesForGroup” “codepipeline：ListPackageGroups” “codepipeline：ListActionTypes” “connect：ListTagsForResource” “截止日期：ListWebhooks” “ec2：” “ec2：DescribeTrafficDistributionGroup” “ec2：” ListTrafficDistributionGroups ListFarms GetTransitGatewayRouteTablePropagations SearchLocalGatewayRoutesSearchTransitGatewayMulticastGroups” “实体分辨率：” “实体分辨率：GetMatchingWorkflow”	该政策现在支持、、Amazon Bedrock Amazon Amplify、Amazon AppSync、、、、、Amazon Connect Amazon CloudTrail Amazon CloudFormation Amazon CodeArtifact、 Amazon CodePipeline、、、亚马逊、、 Amazon Deadline Cloud、、亚马逊 EC2、Amazon Entity Resolution 数据匹配服务 Amazon IoT SiteWise、Amazon Quick Suite、 Amazon Lambda A EventBridge mazon Redshift、Serverless、、、亚马逊 Amazon Identity and Access Management Roles Anywhere、、、 SageMaker 亚马逊安全湖 Amazon Service Catalog、、、 Amazon Secrets Manager、Amazon Systems Manager 和。Amazon Shield EC2 Amazon WAFV2	2025 年 10 月 1 日

更改	描述	日期
“iotsitewise：” “iotsitewise：ListMatchingWorkflows” “iotsitewise：” “iotsitewise：ListAssetModelCompositeModels” “iotsitewise：ListAssetModelProperties” “ivs：” “lambda：” “lambda：” “lambda：ListAssetProperties” “pipes：” “pipes：ListAssociatedAssets” “quicksight：” “quicksight：ListPublicKeys” “redshift-serverlessift：GetRuntimeManagementConfig” “redshift：” “redshift：ListFunctionEventInvokeConfigs” “redshift：ListFunctionUrlConfigs”:” “rolesanywhere：DescribePipe” “rolesanywhere：ListPipes” “sagemaker：DescribeRefreshSchedule” “sagemaker：” “sagemaker：ListRefreshSchedules” “sagemaker：” “GetProvisionedConcurrencyConfigListSnapshotCopyConfigurationsGetResourcePolicyGetCrlListCrlsDescribeAppDescribeUserProfileListApps” “sagemaker：ListModelPackages” “sagemaker：” “securitymanager：ListUserProfiles” “securitylake：GetResourcePolicy” “servicecatalog：ListSubscribersListTagsForResource”		

更改	描述	日期
“servicecatalog：” “ssemcata log：DescribeServiceAction” “ssm：” ssm：“ssm：ListAppli cations” “ssm：” “ssm： ListAssociatedResources” “ssm：ListProtectionGroups” “ssm：ListTagsForResource”:” “ssm：” “ssm：GetReplicatio nSet” “wafv2：” “bedrock-agentcore：ListReplicationSe ts” “bedro DescribeAssociatio n ck-agentcore：Descr ibePatchBaselines” “bedrock-agentcore：GetDefau ltPatchBaseline” “bedrock GetPatchBaseline GetResour cePolicies ListAssociations ListResourceDataSync ListLoggingConfigurations ListCodeInterpreters GetCodeInterpreter-agentcor e：” “bedrock-agentcore ：ListBrowsers” “bedrock-agentcore：” “bedrock-agentcore：GetBrows er” “bedrock-agentcore ：” “bedrock-agentcore：” “bedrock-agentcore：ListAgen tRuntimes” GetAgentRuntime ListAgentRuntimeEndpoints GetAgentRuntimeEndpoint		

更改	描述	日期
AWSConfigServiceRolePolicy— 添加 “放大：” “放大：GetDomainAssociation” “放大：” “appsync：ListDomainAssociations” “appsync：ListTagsForResource” “bedrock：GetSourceApiAssociation” “bedrock：ListSourceApiAssociations” “bedrock：GetFlow” “bedrock：ListAgentCollaborators” “cloudFormation：ListFlows” “codeartifact：ListPrompts” “codeartifact：GetResourcePolicy” “codeartifact：DescribePublisherDescribePackageGroup” “codepipeline：ListAllowedRepositoriesForGroup” “codepipeline：ListPackageGroups” “codepipeline：ListActionTypes” “connect：ListTagsForResource” “截止日期：ListWebhooks” “ec2：” “ec2：DescribeTrafficDistributionGroup” “ec2：” ListTrafficDistributionGroups ListFarms GetTransitGatewayRouteTablePropagations SearchLocalGatewayRoutesSearchTransitGatewayMulticastGroups” “实体分辨率：” “实体分辨率：GetMatchingWorkflow”	该政策现在支持、、Amazon Bedrock Amazon Amplify、Amazon AppSync、、、、、Amazon Connect Amazon CloudTrail Amazon CloudFormation Amazon CodeArtifact、 Amazon CodePipeline、、、亚马逊、、 Amazon Deadline Cloud、、亚马逊 EC2、Amazon Entity Resolution 数据匹配服务 Amazon IoT SiteWise、Amazon Quick Suite、 Amazon Lambda A EventBridge mazon Redshift、Serverless、、、亚马逊 Amazon Identity and Access Management Roles Anywhere、、、 SageMaker 亚马逊安全湖 Amazon Service Catalog、、、 Amazon Secrets Manager、Amazon Systems Manager 和。Amazon Shield EC2 Amazon WAFV2	2025 年 10 月 1 日

更改	描述	日期
“iotsitewise：” “iotsitewise：ListMatchingWorkflows” “iotsitewise：” “iotsitewise：ListAssetModelCompositeModels” “iotsitewise：ListAssetModelProperties” “ivs：” “lambda：” “lambda：” “lambda：ListAssetProperties” “pipes：” “pipes：ListAssociatedAssets” “quicksight：” “quicksight：ListPublicKeys” “redshift-serverlessift：GetRuntimeManagementConfig” “redshift：” “redshift：ListFunctionEventInvokeConfigs” “redshift：ListFunctionUrlConfigs”:” “rolesanywhere：DescribePipe” “rolesanywhere：ListPipes” “sagemaker：DescribeRefreshSchedule” “sagemaker：” “sagemaker：ListRefreshSchedules” “sagemaker：” “GetProvisionedConcurrencyConfigListSnapshotCopyConfigurationsGetResourcePolicyGetCrlListCrlsDescribeAppDescribeUserProfileListApps” “sagemaker：ListModelPackages” “sagemaker：” “securitymanager：ListUserProfiles” “securitylake：GetResourcePolicy” “servicecatalog：ListSubscribersListTagsForResource”		

更改	描述	日期
“servicecatalog：” “ssemcata log：DescribeServiceAction” “ssm：” ssm：“ssm：ListAppli cations” “ssm：” “ssm： ListAssociatedResources” “ssm：ListProtectionGroups” “ssm：ListTagsForResource”:” “ssm：” “ssm：GetReplicatio nSet” “wafv2：” “bedrock-agentcore：ListReplicationSe ts” “bedro DescribeAssociatio n ck-agentcore：Descr ibePatchBaselines” “bedrock-agentcore：GetDefau ltPatchBaseline” “bedrock GetPatchBaseline GetResour cePolicies ListAssociations ListResourceDataSync ListLoggingConfigurations ListCodeInterpreters GetCodeInterpreter-agentcor e：” “bedrock-agentcore ：ListBrowsers” “bedrock-agentcore：” “bedrock-agentcore：GetBrows er” “bedrock-agentcore ：” “bedrock-agentcore：” “bedrock-agentcore：ListAgen tRuntimes” GetAgentRuntime ListAgentRuntimeEndpoints GetAgentRuntimeEndpoint		

更改	描述	日期
AWS_ConfigRole— 添加”arc-zonal-shift：GetAutoshiftObserverNotificationStatus“、“基石：”、“cloudtrail：”、GetModelInvocationLoggingConfiguration “codeartifact：”、GetEventConfiguration “codeartifaction：”、“截止日期：”、DescribeDomain “截止日期：”、“截止日期：”、GetDomainPermissionsPolicy “dms：”、“dms：”、GetFleet “glue：”、GetQueueFleetAssociation “kafkaconnect：”、ListFleets “kafkaconnect：”、ListQueueFleetAssociations “kafkaconnect：”、ListTagsForResource “kafkaconnect：DescribeDataMigrations”、“kafkaconnect：”、“kafkaconnect：”、ListMigrationProjects “kafkaconnect：”、GetDataCatalogEncryptionSettings “kafect：”、“kafkaconnect：DescribeCustomPlugin”、“kafkaconnect：DescribeWorkerConfiguration”、“lakeformation：”、“medialive：”、“medialive：ListCustomPlugins”、“medialive：”、“m ListTagsForResource ListWorke	该政策现在支持亚马逊贝德罗克 Amazon ARC - Zonal Shift、、、、、、、、、Amazon CloudTrail、Amazon CodeArtifact、Amazon Deadline Cloud、、Amazon Database Migration Service Amazon Glue Amazon Identity and Access Management、Amazon Managed Streaming Amazon Lake Formation、、、CloudWatch Amazon AWS Elemental MediaLive Logs AWS Elemental MediaPackage、、、、亚马逊关系数据库服务、亚马逊简单存储服务 Amazon Secrets Manager、、亚马逊安全湖 Amazon Service Catalog、、亚马逊简单电子邮件服务和。 Amazon X-Ray	2025 年 7 月 28 日

更改	描述	日期
rConfigurations DescribeL akeFormationIdentityCenterC onfiguration DescribeM ultiplexProgramListMultiple xPrograms“ , ” mediapack agev2 : ”、“mediapack agev2 : GetChannelGr oup”、“rds : ”、“roles anywhere : ListChann elGroups”、“rolesanywhere : DescribeEngineDefaul tParameters”、“anyw here : ”、“rolesanywhere : GetProfile”、“s3 : ”、“secu ritylake : GetTrustAnchor”、“s ecuritylake : ListProfiles”、“ securitylake : ”、“anywhere : ListTagsForResource” 、“securitylake : ”、ListTrustA nchors “securitylake : GetA ccessGrant”、“securitylake : ListAccessGrants”、“securityl ake : “、“servicecatalog : DescribeSecret”、“servic ecatalog : ListDataLakeExcept ions”、“servicecatalog : ListD ataLakes”、“servicecatalog : ” 、“ses : ListLogSourc es”、“ses : ”、“ses : ”、 “ses : GetAttributeGroup“ , ” ListAttributeGroups ListServi ceActions ListServiceActions ForProvisioningArtifact GetTrafficPolicy ListTagsF orResourceses : ListTrafficPo		

更改	描述	日期
licies“、“xray：”、“xray：GetGroup”、“xray：GetGroups”、“xray：”、“xray：GetSamplingRules”、“xray：”、ListResourcePolicies “xray：” ListTagsForResource		

更改	描述	日期
AWSConfigServiceRolePolicy— 添加 “arc-zonal-shift:”、GetAutoshiftObserverNotificationStatus “基石：”、“cloudtrail：GetModelInvocationLoggingConfiguration”、“codeartifact：GetEventConfiguration”、“codeartifact：DescribeDomain”、“截止日期：”、“截止日期：GetDomainPermissionsPolicy”、“截止日期：”、“dms：GetFleet”、“dms：”、“glue：GetQueueFleetAssociation”、“iam：ListFleets”、“kafkaconnect：ListQueueFleetAssociations”、“kafkaconnect：ListTagsForResource”、“kafkaconnect：DescribeDataMigrations”，“kafkaconnect：ListMigrationProjects”，“kafkaconnect：GetDataCatalogEncryptionSettings”，“kafkaconnect：ListPolicies”，“kafconnect：”、“kafkaconnect：DescribeCustomPlugin”、“kafkaconnect：DescribeWorkerConfiguration”、“lakeformation：”、“logs：”、“logs：ListCustomPlugins”、“logs：”、“logs：ListTags	该政策现在支持对亚马逊 Bedrock Amazon ARC - Zonal Shift、、、、、、Amazon CloudTrail、、Amazon CodeArtifact、Amazon Deadline Cloud、Amazon Database Migration Service Amazon Glue Amazon Identity and Access Management、Amazon Managed Streaming Amazon Lake Formation、、、CloudWatch Amazon L AWS Elemental MediaLive ogs AWS Elemental MediaPackage、、、、、亚马逊关系数据库服务、亚马逊简单存储服务 Amazon Secrets Manager、、亚马逊安全湖 Amazon Service Catalog、亚马逊简单电子邮件 Amazon X-Ray服务和亚马逊 API Gateway 的额外权限。	2025 年 7 月 28 日

更改	描述	日期
ForResource”、“medi alive：ListWorkerConfigurati onsDescribeLakeFor mationIdentityCenterConfigu rationDescribeIndexPolicies ListTagsForResourceDescribe MultiplexProgram“ , ” medialive：ListMultiplexProg rams”、“mediapackag ev2：”、“mediapackag ev2：GetChannelGrou p”、“rds：”、“rolesan ywhere：”、“rolesanywhere： ListChannelGroups”、“r olesanywhere：Descr ibeEngineDefaultParameters” 、“rolesanywhere：”、 “rolesanywhere：”、G etProfile “rolesanywhere： GetTrustAnchor”、“role sanywhere：”、“roles anywhere：”、ListPro files “rolesanywhere： ListTagsForResource”、 “rolesanywhere：”、ListTrustA nchors “rolesanywhere：”、“ “、GetAccessGrant “security lake：ListAccessGrants”、“ser vicecatalog：”、“servicecatal og：DescribeSecret” 、“servicecatalog：ListDataLa keExceptions”、“servicecatal og：”、ListDataLakes “servicecatalog：”、“ses： ListLogSourcesGetAttri		

更改	描述	日期
buteGroupListAttributeGroupsListServiceActionsListServiceActionsForProvisioningArtifactGetTrafficPolicy“、“ses：”、“ses：ListTagsForResource”、“xray：”、“xray：ListTrafficPolicies”、“xray：”、“xray：GetGroup”、“xray：”、“xray：”、GetGroups “arn: aws: apigateway:: /accountGetSamplingRules”、“arn: aws:: /usageplans/”、ListResourcePolicies “arn: aws:: ListTagsForResource /usageplans”、“arn: aws: apigateway:: /usageplans/”。		

更改	描述	日期
AWSConfigServiceRolePolicy— 添加 “backup-gateway：”、GetHypervisor “backup-gatewaybcm-data-exports：”、ListHypervisors GetExport “、”bcm-data-exports：ListExports“、”、“基岩bcm-data-exports：”、ListTagsForResource “基岩：”、“基岩：”、GetAgent “基岩：”、GetAgentActionGroup “基岩：”、“基岩：”、GetAgentKnowledgeBase “基岩：”、“基岩：”、GetDataSource “基岩：”、“基岩：”、GetFlowAlias “基岩：”、GetFlowVersion “基岩：”、“基岩：ListAgentActionGroups”，“cloudformation：ListAgentKnowledgeBases”，“cloudformation：ListDataSources”，“cloudformation：ListFlowVersions”，“cloudformati ListFlowAliases BatchDescribeTypeConfigurations DescribeStackInstance DescribeStackSet ListStackInstancescloudformation：”、ListStackSets “cloudfront：”、GetPublicKey “cloudfront：GetRealtimeLogConfig”、“cloudfront：ListPublicKeys”、“实体分辨率：”、L	该策略现在支持对、、Amazon Bedrock Amazon Backup gateway Amazon 账单与成本管理、、、Amazon、 Amazon CloudFormation、、、CloudFront、、、 Amazon Entity Resolution 数据匹配服务、 Amazon IoT Core Device Advisor、 Amazon Lambda Amazon Network Manager Amazon 私有证书颁发机构、Amazon Redshift、Amazon S3 Tables 等的额外权限。 Amazon Systems Manager 快速设置功能	2025 年 6 月 18 日

更改	描述	日期
istRealtimeLogConfigs “实体分辨率：”、“实体分辨率：”、“实体分辨率：GetIdMappingWorkflow”、“iotdeviceAdvisor：GetSchemaMapping”、“iotdeviceAdvisor：”、ListIdMappingWorkflows “iotdeviceAdvisor：”、ListSchemaMappings “lambda：ListTagsForResource”、“lambda：” , “” mediapackagev2：GetSuiteDefinition“ , ” mediapackagev2：ListSuiteDefinitions“ , ” networkmanager：GetEventSourceMapping“ , ” networkmanager：ListEventSourceMappings“ , ” : “ , ” GetChannel ListChannels GetTransitGatewayPeering ListPeeringspca-connector-ad GetDirectoryRegistrationpca-connector-ad: ListDirectoryRegistrations“,”: “、“rdspca-connector-ad: ListTagsForResource Describe G DBShardroups”、“rds:”、“redshift：DescribeIntegrations”、“s3tables：”、“s3tables：”、DescribeIntegrations “s3tables：”、“s3tables：”、GetTableBucket “ssm-quicksetup：”、GetTableBucketEncryption “ssm-quic		

更改	描述	日期
ksetup：”，GetTableBucketMaintenanceConfiguration“ssm-quicksetup：” ListTableBuckets GetConfigurationManager ListConfigurationManagers		

更改	描述	日期
AWS_ConfigRole— 添加 “backup-gateway：”、GetHypervisor “backup-gatewaybcm-data-exports：”、ListHypervisors GetExport “、”bcm-data-exports：ListExports“、”、“基岩bcm-data-exports：”、ListTagsForResource “基岩：”、“基岩：”、GetAgent “基岩：”、GetAgentActionGroup “基岩：”、“基岩：”、GetAgentKnowledgeBase “基岩：”、“基岩：”、GetDataSource “基岩：”、“基岩：”、GetFlowAlias “基岩：”、GetFlowVersion “基岩：”、“基岩：ListAgentActionGroups”，“cloudformation：ListAgentKnowledgeBases”，“cloudformation：ListDataSources”，“cloudformation：ListFlowVersions”，“cloudformati ListFlowAliases BatchDescribeTypeConfigurations DescribeStackInstance DescribeStackSet ListStackInstances cloudformation：”、ListStackSets “cloudfront：”、GetPublicKey “cloudfront：”、GetRealtimeLogConfig “cloudfront：”、ListPublicKeys “实	该策略现在支持对、、Amazon Bedrock Amazon Backup gateway Amazon 账单与成本管理、、、Amazon、 Amazon CloudFormation、、、CloudFront、、、 Amazon Entity Resolution 数据匹配服务、 Amazon IoT Core Device Advisor、 Amazon Lambda Amazon Network Manager Amazon 私有证书颁发机构、Amazon Redshift、Amazon S3 Tables 等的额外权限。Amazon Systems Manager 快速设置功能	2025 年 6 月 18 日

更改	描述	日期
体分辨率：ListRealtim eLogConfigs”、“实体分辨率：”、“实体分辨率：GetIdMa ppingWorkflow”、“实体分辨率：”、GetSchemaMap ping “iotdeviceAdvisor：”、ListIdMappingWorkflows “iotdeviceAdvisor：ListSchem aMappings”、“iotdeviceAdviso r：ListTagsForResou rce”、“lambda：”、“lambda：GetSuiteDefinition”，“” networkmanager：Lis tSuiteDefinitions“，”，“netwo rkmanager：”，GetEve ntSourceMapping”：“，”：“，”：ListEventSo urceMappings“，” rds：GetTransitGatewayPeerin gListPeeringspca-connector-adGetDirectoryRegistrationpca-connector-adListDirectoryRegistrationspca-connector-adListTagsForResource描述DBShard群组”、“rds：”、“redshift：”、DescribeIntegratio ns “s3tables：”、“s3tab les：”、DescribeInte grations “s3tables：”、“s3tab les：”、GetTableBuck et “s3tables：”、GetTab leBucketEncryption “ssm-quicksetup：”、“ssm-quic ksetup：”、GetTableB ucketMaintenanceConfigurati		

更改	描述	日期
on “ssm-quickset ListTable Buckets up：”，GetConfigurationManagerListConfiguration Managers		
AWS_ConfigRole – 添加 "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails"，" bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases"，"bedrock:ListTagsForResource"	此策略现在支持为 Amazon Bedrock 授予更多权限。	2025 年 5 月 27 日
AWSConfigServiceRolePolicy – 添加 "bedrock:GetGuardrail", "bedrock:GetInferenceProfile", "bedrock:GetKnowledgeBase", "bedrock:ListGuardrails"，" bedrock:ListInferenceProfiles", "bedrock:ListKnowledgeBases"，"bedrock:ListTagsForResource"	此策略现在支持为 Amazon Bedrock 授予更多权限。	2025 年 5 月 27 日

更改	描述	日期
AWS_ConfigRole – 添加 "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	该政策现在支持对亚马逊 Bedrock Amazon B2B Data Interchange、、、、、 Amazon Database Migration Service（Amazon DMS）、Amazon L CloudWatch ogs Amazon Clean Rooms Amazon CodeConnections Amazon Direct Connect、Amazon Macie、Amazon Managed Blockchain、Amazon Q Business、Route 53 Profiles、亚马逊简单存储服务 (Amazon S3)、Amazon A SageMaker I Amazon Security Hub CSPM、 Amazon Systems Manager Incident Manager以及联系人等的额外权限。 Amazon Systems Manager Incident Manager Amazon Systems Manager	2025 年 4 月 8 日

更改	描述	日期
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsForResource", "s3:GetAccessGrantsInstance", "s3:GetAccessGrantsLocation", "s3:ListAccessGrantsInstances", "s3:ListAccessGrantsLocations", "sagemaker:DescribeCluster", "sagemaker:DescribeMlflowTrackingServer", "sagemaker:DescribeStudioLifecycleConfig", "sagemaker:ListClusters", "sagemaker:ListMlflowTrackingServers", "sagemaker:ListStudioLifecycleConfigs", "securityhub:DescribeStandardsControls", "securityhub:GetEnabledStandards", "ssm-contacts:GetContact", "ssm-contacts:GetContactChannel", "ssm-contacts:ListContactChannels", "ssm-contacts:ListContacts", "ssm-incidents:GetResponsePlan", "ssm-incidents:ListResponsePlans", "ssm-incidents:ListTagsForResource", "ssm:DescribeInstanceInformation"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "b2bi:GetPartnership", "b2bi:GetProfile", "b2bi:ListPartnerships", "b2bi:ListProfiles", "bedrock:ListAgents", "cleanrooms:GetConfiguredTable", "cleanrooms:GetConfiguredTableAnalysisRule", "cleanrooms:GetMembership", "cleanrooms:GetPrivacyBudgetTemplate", "cleanrooms:ListConfiguredTables", "cleanrooms:ListMemberships", "cleanrooms:ListPrivacyBudgetTemplates", "codeconnections:GetConnection", "codeconnections:ListConnections", "codeconnections:ListTagsForResource", "directconnect:DescribeConnections", "dms:DescribeReplicationConfigs", "logs:DescribeAccountPolicies", "logs:DescribeResourcePolicies", "macie2:ListAutomatedDiscoveryAccounts", "managedblockchain:GetAccessor", "managedblockchain:ListAccessors", "qbusiness:GetApplication", "qbusiness:ListApplications", "qbusiness:ListTagsForResource", "route53profiles:GetProfile", "route53profiles:GetProfileAssociation", "route53profi	该政策现在支持对亚马逊 Bedrock Amazon B2B Data Interchange、、、、、 Amazon Database Migration Service（Amazon DMS）、Amazon L CloudWatch ogs Amazon Clean Rooms Amazon CodeConnections Amazon Direct Connect、Amazon Macie、Amazon Managed Blockchain、Amazon Q Business、Route 53 Profiles、亚马逊简单存储服务 (Amazon S3)、Amazon A SageMaker I Amazon Security Hub CSPM、Amazon Systems Manager Incident Manager以及联系人等的额外权限。 Amazon Systems Manager Incident Manager Amazon Systems Manager此策略现在还支持通过包含资源模式“`arn:aws:apigateway:::/domainnames/` ”来访问所有 Amazon API Gateway 域名的权限。	2025 年 4 月 8 日

更改	描述	日期
les:ListProfileAssociations", "route53profiles:ListProfiles", "route53profiles:ListTagsFor Resource", "s3:GetAccessGra ntsInstance", "s3:GetAc cessGrantsLocation", "s3:Li stAccessGrantsInstances", "s3:ListAccessGrantsLocatio ns", "sagemaker:DescribeClu ster", "sagemaker:DescribeM lflowTrackingServer", "sage maker:DescribeStudioLifecyc leConfig", "sagemaker:ListC lusters", "sagemaker:ListMlf lowTrackingServers", "sagem aker:ListStudioLifecycleCon figs", "securityhub:Describ eStandardsControls", "secur ityhub:GetEnabledStandards" , "ssm-contacts:GetContact", "ssm-contacts:GetContactCha nnel", "ssm-contacts:ListCo ntactChannels", "ssm-cont acts:ListContacts", "ssm-in cidents:GetResponsePlan", " ssm-incidents:ListResponseP lans", "ssm-incidents:ListT agsForResource", "ssm:Descr ibeInstanceInformation"		
AWS_ConfigRole – 添加 "ec2:GetAllowedImagesSettin gs"	该策略现在支持亚马逊弹性计算云 (Amazon EC2) 的额外权限。	2025 年 3 月 4 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "ec2:GetAllowedImagesSettings"	该策略现在支持亚马逊弹性计算云 (Amazon EC2) 的额外权限。	2025 年 3 月 4 日
AWS_ConfigRole – 添加 "cleanrooms-ml:GetTrainingDataset", "cleanrooms-ml:ListTrainingDatasets", "comprehend:DescribeFlywheel", "comprehend:ListFlywheels", "comprehend:ListTagsForResource", "ec2:GetSnapshotBlockPublicAccessState", "omics:GetAnnotationStore", "omics:GetRunGroup", "omics:GetSequenceStore", "omics:GetVariantStore", "omics:ListAnnotationStores", "omics:ListRunGroups", "omics:ListSequenceStores", "omics:ListTagsForResource", "omics:ListVariantStores", "s3express:GetEncryptionConfiguration", "s3express:GetLifecycleConfiguration", "ses:GetDedicatedIpPool", "ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	该政策现在支持亚马逊 Comprehend Amazon Clean Rooms、亚马逊弹性计算云 EC2（亚马逊）、亚马逊简单存储服务（Amazon S3 Amazon HealthOmics）和亚马逊简单电子邮件服务（Amazon SES）的额外权限。	2025 年 1 月 16 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "cleanrooms-ml:GetTrainingDataset"，"cleanrooms-ml:ListTrainingDatasets"，"comprehend:DescribeFlywheel", "comprehend:ListFlywheels"，"comprehend:ListTagsForResource"，"ec2:GetSnapshotBlockPublicAccessState"，"omics:GetAnnotationStore", "omics:GetRunGroup"，"omics:GetSequenceStore"，"omics:GetVariantStore"，"omics:ListAnnotationStores"，"omics:ListRunGroups"，"omics:ListSequenceStores"，"omics:ListTagsForResource"，"omics:ListVariantStores"，"s3express:GetEncryptionConfiguration"，"s3express:GetLifecycleConfiguration"，"ses:GetDedicatedIpPool"，"ses:GetDedicatedIps", and "ses:ListDedicatedIpPools"	该政策现在支持亚马逊 Comprehend Amazon Clean Rooms、亚马逊弹性计算云 EC2（亚马逊）、亚马逊简单存储服务（Amazon S3 Amazon HealthOmics）和亚马逊简单电子邮件服务（Amazon SES）的额外权限。	2025 年 1 月 16 日
AWSConfigServiceRolePolicy – 添加 "organizations:ListAWSServiceAccessForOrganization"	此策略现在支持为 Amazon Organizations授予更多权限。	2024 年 12 月 18 日

更改	描述	日期
AWS_ConfigRole – 添加 "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType", "iot:ListThingGroups", "iot	该政策现在支持、、Amazon Connect Amazon AppConfig Amazon CloudTrail、Amazon、Amazon DevOps Guru DataZone、、Identity Store Amazon Glue、、、、Amazon IoT Amazon IoT FleetWise Amazon IoT Wireless、亚马逊互动视频服务 (Amazon IVS)、亚马逊 CloudWatch 日志、亚马逊可观察性访问管理器、、亚马逊关系 Amazon Payment Cryptography数据库服务 (Amazon RDS)、 CloudWatch Amazon Rekognition、亚马逊简单存储服务 (Amazon S3) 的额外权限 Service S3S、Amazon Scheduler 和 Amazon VPC Lattice。EventBridge Amazon Systems Manager	2024 年 11 月 7 日

更改	描述	日期
:ListThingTypes", "iotfleetwise:GetDecoderManifest", "iotfleetwise:GetFleet", "iotfleetwise:GetModelManifest", "iotfleetwise:GetSignalCatalog", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderManifestNetworkInterfaces", "iotfleetwise:ListDecoderManifests", "iotfleetwise:ListDecoderManifestSignals", "iotfleetwise:ListFleets", "iotfleetwise:ListModelManifestNodes", "iotfleetwise:ListModelManifests", "iotfleetwise:ListSignalCatalogNodes", "iotfleetwise:ListSignalCatalogs", "iotfleetwise:ListTagsForResource", "iotfleetwise:ListVehicles", "iotwireless:GetDestination", "iotwireless:GetDeviceProfile", "iotwireless:GetWirelessGateway", "iotwireless:ListDestinations", "iotwireless:ListDeviceProfiles", "iotwireless:ListWirelessGateways", "ivschat:GetLoggingConfiguration", "ivschat:GetRoom" "ivschat:ListLoggingConfigurations", "ivschat:ListRooms", "ivschat:ListTagsForResource", "logs:GetLogAnomalyDetector", "logs:ListLogAnomalyDetectors", "oam:GetS		

更改	描述	日期
ink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "app-integrations:GetApplication", "app-integrations:ListApplications", "app-integrations:ListTagsForResource", "appconfig:GetExtension", "appconfig:ListExtensions", "cloudtrail:GetInsightSelectors", "connect:DescribeQueue", "connect:DescribeRoutingProfile", "connect:DescribeSecurityProfile", "connect:ListQueueQuickConnects", "connect:ListQueues", "connect:ListRoutingProfileQueues", "connect:ListRoutingProfiles", "connect:ListSecurityProfileApplications", "connect:ListSecurityProfilePermissions", "connect:ListSecurityProfiles", "datazone:GetDomain", "datazone:ListDomains", "devops-guru:ListNotificationChannels", "glue:GetRegistry", "glue:ListRegistries", "identitystore:DescribeGroup", "identitystore:DescribeGroupMembership" "identitystore:ListGroupMemberships", "identitystore:ListGroups", "iot:DescribeThingGroup", "iot:DescribeThingType",	该政策现在支持、、Amazon Connect Amazon AppConfig Amazon CloudTrail、Amazon、Amazon DevOps Guru DataZone、、Identity Store Amazon Glue、、、、Amazon IoT Amazon IoT FleetWise Amazon IoT Wireless、亚马逊互动视频服务 (Amazon IVS)、亚马逊 CloudWatch 日志、亚马逊可观察性访问管理器、、亚马逊关系 Amazon Payment Cryptography数据库服务 (Amazon RDS)、 CloudWatch Amazon Rekognition、亚马逊简单存储服务 (Amazon S3) 的额外权限 Service S3S、Amazon Scheduler 和 Amazon VPC Lattice。EventBridge Amazon Systems Manager	2024 年 11 月 7 日

更改	描述	日期
"iot:ListThingGroups", "iot :ListThingTypes", "iotfleet wise:GetDecoderManifest", " iotfleetwise:GetFleet", "iotfleet wise:GetModelManifest", "io tfleetwise:GetSignalCatalog ", "iotfleetwise:GetVehicle", "iotfleetwise:ListDecoderMa nifestNetworkInterfaces", " iotfleetwise:ListDecoderMan ifests", "iotfleetwise:List DecoderManifestSignals", "iotfleetwise:ListFleets", "i otfleetwise:ListModelManife stNodes", "iotfleetwise:Lis tModelManifests", "iotfleet wise:ListSignalCatalogNodes ", "iotfleetwise:ListSignal Catalogs", "iotfleetwise:Li stTagsForResource", "iotfleet wise:ListVehicles", "iotwir eless:GetDestination", "iotwirel ess:GetDeviceProfile", "iot wireless:GetWirelessGateway ", "iotwireless:ListDestina tions", "iotwireless:ListDe viceProfiles", "iotwireless :ListWirelessGateways", "iv schat:GetLoggingConfigurati on", "ivschat:GetRoom" "ivschat:ListLoggingConfigu rations", "ivschat:ListRooms ", "ivschat:ListTagsForReso urce", "logs:GetLogAnomal yDetector", "logs:ListLogAn		

更改	描述	日期
omalyDetectors", "oam:GetSink" "oam:GetSinkPolicy", "oam:ListSinks", "payment-cryptography:GetAlias", "payment-cryptography:GetKey", "payment-cryptography:ListAliases", "payment-cryptography:ListKeys", "payment-cryptography:ListTagsForResource", "rds:DescribeDBProxyTargetGroups", "rds:DescribeDBProxyTargets", "rekognition:DescribeProjects", "s3:GetStorageLensGroup", "s3:ListStorageLensGroups", "s3:ListTagsForResource", "scheduler:GetScheduleGroup", "scheduler:ListScheduleGroups", "scheduler:ListTagsForResource", "ssm:GetServiceSetting", "vpc-lattice:GetAccessLogSubscription", "vpc-lattice:GetService", "vpc-lattice:GetServiceNetwork", "vpc-lattice:GetTargetGroup", "vpc-lattice:ListAccessLogSubscriptions", "vpc-lattice:ListServiceNetworks", "vpc-lattice:ListServices", "vpc-lattice:ListTagsForResource", "vpc-lattice:ListTargetGroups", and "vpc-lattice:ListTargets"		

更改	描述	日期
AWS_ConfigRole – 添加 "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	该政策现在支持亚马逊 OpenSearch 服务 Severless 、、、、、、Im EC2 age Builder AppStream、 Amazon Backup Amazon CloudTrail Amazon Glue、Amazon Interactive Video Service (Amazon IVS)、、、 AWS Elemental MediaConnect AWS Elemental MediaTailor、 Amazon HealthOmics和 Amazon Scheduler 的额外权限。 Amazon IoT EventBridge	2024 年 9 月 16 日

更改	描述	日期
rictionPolicies," "ivs:List Stages," "ivs:ListStorageCo nfigurations," "mediacon nect:DescribeBridge", "medi aconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChanne l," "mediatailor:DescribeLi veSource," "mediatailor:Des cribeSourceLocation," "medi atailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSourc es", "mediatailor:ListSourc eLocations," "mediatailor:ListV odSources," "omics:GetWorkf low," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "aoss:BatchGetCollection," "aoss:BatchGetLifecyclePolicy," "aoss:BatchGetVpcEndpoint," "aoss:GetAccessPolicy," "aoss:GetSecurityConfig," "aoss:GetSecurityPolicy," "aoss:ListAccessPolicies," "aoss:ListCollections," "aoss:ListLifecyclePolicies," "aoss:ListSecurityConfigs," "aoss:ListSecurityPolicies," "aoss:ListVpcEndpoints," "appstream:DescribeAppBlockBuilders," "backup:GetRestoreTestingPlan," "backup:GetRestoreTestingSelection", "backup:ListRestoreTestingPlans," "backup:ListRestoreTestingSelections," "cloudTrail:GetChannel, "cloudTrail:ListChannels," "glue:GetTrigger," "glue:ListTriggers, "imagebuilder:GetLifecyclePolicy," "imagebuilder:ListLifecyclePolicies," "iot:DescribeBillingGroup, " "iot:ListBillingGroups," "ivs:GetEncoderConfiguration, " "ivs:GetPlaybackRestrictionPolicy," "ivs:GetStage," "ivs:GetStorageConfiguration, " "ivs:ListEncoderConfigurations," "ivs:ListPlaybackRest	该政策现在支持亚马逊 OpenSearch 服务 Severless 、、、、、、Im EC2 age Builder AppStream、 Amazon Backup Amazon CloudTrail Amazon Glue、Amazon Interactive Video Service (Amazon IVS)、、、 AWS Elemental MediaConnect AWS Elemental MediaTailor、 Amazon HealthOmics和 Amazon Scheduler 的额外权限。 Amazon IoT EventBridge	2024 年 9 月 16 日

更改	描述	日期
rictionPolicies," "ivs:List Stages," "ivs:ListStorageCo nfigurations," "mediacon nect:DescribeBridge", "medi aconnect:DescribeGatewa," "mediaconnect:ListBridges," "mediaconnect:ListGateways", "mediatailor:DescribeChanne l," "mediatailor:DescribeLi veSource," "mediatailor:Des cribeSourceLocation," "medi atailor:DescribeVodSource", "mediatailor:ListChannels," "mediatailor:ListLiveSourc es", "mediatailor:ListSourc eLocations," "mediatailor:ListV odSources," "omics:GetWorkf low," "omics:ListWorkflows," "scheduler:GetSchedule," and "scheduler:ListSchedules"		
AWS_ConfigRole – 添加 "elasticfilesystem:Describe Tags," "redshift:DescribeTa gs," and "ssm-sap:ListTagsF orResource"	该政策现在支持亚马逊弹性文件系统（亚马逊 EFS）、亚马逊 Redshift 和。 适用于 SAP 的 Amazon Systems Manager	2024 年 6 月 17 日
AWSConfigServiceRolePolicy – 添加 "elasticfilesystem :DescribeTags," "redshift:D escribeTags," and "ssm-sap: ListTagsForResource"	该政策现在支持亚马逊弹性文件系统（亚马逊 EFS）、亚马逊 Redshift 和。 适用于 SAP 的 Amazon Systems Manager	2024 年 6 月 17 日

更改	描述	日期
AWS_ConfigRole – 添加 "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool," "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:G	该政策现在支持亚马逊托管服务 Prometheus、亚马逊、亚马逊 Cognito、亚马逊、亚马逊、（IAM）CloudWatch、、、、Amazon Redshift Serverless、Amazon AI 和 ElastiCache亚马逊简单通知服务（FSxAmaz Amazon Glue on Amazon Identity and Access Management SNS) Simple Notificati Amazon RAM on Serverless Amazon Lambda、Amazon AI 和亚马逊简单通知服务（SageMaker Amazon SNS) 的额外权限。	2024 年 2 月 22 日

更改	描述	日期
etSMSSandboxAccoun tStatus"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "aps:DescribeAlert ManagerDefinition," "cloudwa tch:DescribeAlarmsForMetric ," "cognito-identity:Describ eIdentityPool, "cognito-iden tity:GetPrincipalTagAttribu teMap," "elasticache:Describ eCacheSecurityGroups," "elas ticache:DescribeUserGroups, " "elasticache:DescribeUsers, " "elasticache:DescribeGloba lReplicationGroups," "fsx:De scribeDataRepositoryAssocia tions," "glue:GetDatabase, " "glue:GetDatabases," "iam:ListUsers," "lambda:G etLayerVersion," "lambda:Lis tLayers," "lambda:ListLayerV ersions," "ram:GetPermission ," "ram:ListPermissionAssociat ions," "ram:ListPermissions," "ram:ListPermissionVersions ," "redshift-serverless:GetN amespace," "redshift-serverl ess:GetWorkgroup," "redshift -serverless:ListNamespaces, " "redshift-serverless:ListT agsForResource," "redshift-s erverless:ListWorkgroups," " sagemaker:DescribeInference Experiment," "sagemaker:List InferenceExperiments," and	该政策现在支持亚马逊托管服务 Prometheus、亚马逊、亚马逊 Cognito、亚马逊、亚马逊、（IAM）CloudWatc h、、、、Amazon Redshift Serverless、Amazon AI 和 ElastiCache亚马逊简单通知服务（FSxAmaz Amazon Glue on Amazon Identity and Access Management SNS) Simple Notificati Amazon RAM on Serverless Amazon Lambda、Amazon AI 和亚马逊简单通知服务（SageMaker Amazon SNS) 的额外权限。	2024 年 2 月 22 日

更改	描述	日期
"sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess—Amazon Config 开始跟踪此 Amazon 托管策略的更改	此政策提供使用权限 Amazon Config，包括按资源标签搜索和读取所有标签。这不提供配置权限 Amazon Config，而配置权限需要管理权限。	2024 年 2 月 22 日
AWS_ConfigRole – 添加 "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	该政策现在支持适用于 Prometheus 的亚马逊托管服务 Amazon AppConfig、Amazon DMS()、() IAM Amazon Database Migration Service 、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK Amazon Identity and Access Management）、亚马逊 Amazon Organizations日志和亚马逊简单存储服务 (Amazon S3) Simple Storage Service 的额外权限。 CloudWatch	2023 年 12 月 5 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	该政策现在支持适用于 Prometheus 的亚马逊托管服务 Amazon AppConfig、Amazon DMS()、() IAM Amazon Database Migration Service 、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK Amazon Identity and Access Management ）、亚马逊 Amazon Organizations日志和亚马逊简单存储服务 (Amazon S3) Simple Storage Service 的额外权限。 CloudWatch	2023 年 12 月 5 日

更改	描述	日期
AWS_ConfigRole – 添加 "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationAssociation	该政策现在支持亚马逊 Cognito、Amazon Connect、亚马逊 EMR、、、Amazon MemoryDB、 Amazon Ground Station、 Amazon Mainframe Modernization Amazon Quick Suite Amazon Organizations、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Redshift、亚马逊 Rodshift、Amazon Route 53 和。 Amazon Service Catalog Amazon Transfer Family	2023 年 11 月 17 日

更改	描述	日期
s," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrL		

更改	描述	日期
ocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole – 添加 "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	此策略现在为 AWSConfigServiceRolePolicyStatementID AWSConfigSLRLogStatementID 、AWSConfigSLRLogEventStatementID 和 AWSConfigSLRApiGatewayStatementID 添加了安全标识符（SID）。	2023 年 11 月 17 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect	该政策现在支持亚马逊 Cognito、Amazon Connect、亚马逊 EMR、、、Amazon MemoryDB、 Amazon Ground Station、 Amazon Mainframe Modernization Amazon Quick Suite Amazon Organizations、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Redshift、亚马逊 Rodshift、Amazon Route 53 和。 Amazon Service Catalog Amazon Transfer Family	2023 年 11 月 17 日

更改	描述	日期
:ListIntegrationAssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCid		

更改	描述	日期
rBlocks," "route53:ListCidrLocations," "serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy – 添加 "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	此策略现在为 `AWSConfigServiceRolePolicyStatementID` `AWSConfigSLRLogStatementID` 、`AWSConfigSLRLogEventStatementID` 和 `AWSConfigSLRApiGatewayStatementID` 添加了安全标识符（SID）。	2023 年 11 月 17 日

更改	描述	日期
AWS_ConfigRole – 添加 "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListT	该政策现在支持、、Amazon Connect Amazon 私有 CA Amazon App Mesh、亚马逊弹性容器服务 (Amazon ECS)、Amazon Evicently、Ama CloudWatch zon Managed Grafana、亚马逊、Amazon Insp Amazon IoT TwinMaker ector、GuardDuty、、、Amazon Kafka Managed Streaming （ Amazon IoT亚马逊 MSK ）、、、和亚马逊人工智能的额外权限。 Amazon Lambda Amazon Network Manager Amazon Organizations SageMaker	2023 年 10 月 4 日

更改	描述	日期
ags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSi	该政策现在支持、、Amazon Connect Amazon 私有 CA Amazon App Mesh、亚马逊弹性容器服务 (Amazon ECS)、Amazon Evicently 、Ama CloudWatch zon Managed Grafana、亚马逊、Amazon Insp Amazon IoT TwinMaker ector、GuardDuty、、、Amazon Kafka Managed Streaming （ Amazon IoT亚马逊 MSK ）、、、和亚马逊人工智能的额外权限。 Amazon Lambda Amazon Network Manager Amazon Organizations SageMaker	2023 年 10 月 4 日

更改	描述	日期
gningConfigs," "lambda:ListTags," "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy – 移除 "ssm:GetParameter"	此策略现在会移除 Amazon Systems Manager（Systems Manager）的权限。	2023 年 9 月 6 日

更改	描述	日期
AWS_ConfigRole – 添加 "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	该政策现在支持、、亚马逊、、、Amazon Connect Amazon App Mesh Amazon CloudFormation、、亚马逊 CloudFront Amazon CodeArtifact Amazon CodeBuild、Amazon Identity and Access Management (IAM) Amazon Glue、Amazon Inspector GuardDuty、、、、Amazon Inspector Amazon IoT、Amazon IoT TwinMaker 、、 Amazon IoT Wireless、、Amazon Macie、、、、、Amazon Route 53、亚马逊简单存储服务 (Amazon S3) AWS Elemental MediaConnect Amazon Network Manager Amazon Organizations Amazon 资源探索器、亚马逊简单存储服务 (Amazon S3) 和亚马逊简单通知服务 (Amazon SNS) 的额外权限) Simple Service Amazon。	2023 年 7 月 28 日

更改	描述	日期
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSe	该政策现在支持亚马逊 WorkSpaces 应用程序 Amazon App Mesh、、亚马逊、、、、、Amazon Connect CloudFront Amazon CodeArtifact、 Amazon CodeBuild、亚马逊、 Amazon Glue Amazon Identity and Access Management (IAM) GuardDuty、Amazon Inspector、、 Amazon IoT、Amazon IoT TwinMaker 、 Amazon IoT Wireless、Amazon Macie、、、、、、Amazon Route 53 AWS Elemental MediaConnect Amazon Network Manager Amazon Organizations、Amazon 资源探索器亚马逊简单存储服务 (Amazon S3)、亚马逊简单通知服务的额外权限（亚马逊 SNS）Service 和亚马逊 Systems Manager (SSM)。 Amazon CloudFormation EC2	2023 年 7 月 28 日

更改	描述	日期
crets", "macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

更改	描述	日期
AWS_ConfigRole – 添加 "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", “dynamodb:DescribeTableReplicaAutoScaling" "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	该政策现在支持 Amazon Connect Amazon Amplify、、Prometheus 的亚马逊托管服务 Amazon App Mesh、亚马逊 Athena、、、、、、、、、、亚马逊、、、亚马逊 DynamoDB Amazon CloudFormation、亚马逊弹性计算云（亚马逊 CodeGuru） Amazon CloudTrail Amazon CodeArtifact、 Amazon Batch Amazon Evicently、Amazon Forecast、、（ Amazon Identity and Access Management IAM ）CloudWatch 、A EC2 mazon M Amazon IoT Greengrass anaged Streaming 的额外权限 Kafka（ Amazon Ground Station亚马逊 MSK ）、亚马逊 Lightsail 、Amazon Logs、、、Amazon Pinpoint、亚马逊虚拟私有云（ Amazon Directory Service Amazon Organizations CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor亚马逊 VPC)、Amazon Personalize、Amazon Quick Suite Amazon Migration Hub Refactor Spaces、亚马逊简单存储服务 (Amazon S3)、Amazon AI、A	2023 年 6 月 13 日

更改	描述	日期
tasetGroup", "forecast :ListDatasetGroups", "greeng rass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVe rsions", "groundstation:GetM issionProfile", "groundstati on:ListMissionProfiles", "iam:ListGroups", "iam:ListR oles", "kafka:DescribeCon figuration", "kafka:Describe ConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDat abases" "logs:ListTagsLogG roup", "mediaconnec t:DescribeFlow", "mediacon nect:ListFlows", "mediatailo r:GetPlaybackConfiguration" , "mediatailor:ListPlaybackC onfigurations", "mobiletarge ting:GetApplicationSettings ", "mobiletargeting:GetEmail Template", "mobiletargeting: GetEventStream", "mobileta rgeting:ListTemplates", "networkmanager:GetCus tomerGatewayAssociations", "networkmanager:Get LinkAssociations", "organiza tions:DescribeAccount", "organizations:Describ eOrganizationalUnit", "organ izations:ListAccounts",	SageMaker mazon AI 等。Amazon Transfer Family	

更改	描述	日期
"organizations:ListAccounts ForParent", "organizations:L istOrganizationalUnitsForPa rent", "organizations:ListTa gsForResource", "personal ize:DescribeDataset", "perso nalize:DescribeDatasetGroup", "personalize:DescribeSchema ", "personalize:DescribeSolu tion", "personalize:ListD atasetGroups", "personalize: ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForRe source", "quicksight:ListTe mplates", "refactor-spaces:G etEnvironment", "refactor -spaces:GetService", "refactor-spaces:ListAppl ications", "refactor-spaces: ListEnvironments", "refactor -spaces:ListServices", "s3:GetAccessPointPolic yStatusForObjectLambda", "sagemaker:DescribeDe viceFleet", "sagemake r:DescribeFeatureGroup", "sa gemaker:ListDeviceFleets", "sagemaker:ListFeatureGroup s", "sagemaker:ListModels", and "transfer:ListTags ForResource"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	该政策现在支持 Amazon Connect Amazon Amplify、、Prometheus 的亚马逊托管服务 Amazon App Mesh、亚马逊 Athena、、、、、、、、、、亚马逊、、、亚马逊 DynamoDB Amazon CloudFormation、亚马逊弹性计算云（亚马逊 CodeGuru） Amazon CloudTrail Amazon CodeArtifact、 Amazon Batch Amazon Evicently、Amazon Forecast、、（ Amazon Identity and Access Management IAM）CloudWatch 、A EC2 mazon M Amazon IoT Greengrass anaged Streaming 的额外权限 Kafka（ Amazon Ground Station亚马逊 MSK）、亚马逊 Lightsail、Amazon Logs、、、Amazon Pinpoint、亚马逊虚拟私有云（ Amazon Directory Service Amazon Organizations CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor亚马逊 VPC)、Amazon Personalize、Amazon Quick Suite Amazon Migration Hub Refactor Spaces、亚马逊简单存储服务 (Amazon S3)、Amazon AI、A	2023 年 6 月 13 日

更改	描述	日期
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAccounts	SageMaker mazon AI 等。Amazon Transfer Family	

更改	描述	日期
ForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	该政策现在支持亚马逊托管工作流程的额外权限，包括、、、亚马逊 Amazon Amplify、、亚马逊弹性计算云 Amazon App Mesh Amazon App Runner CloudFront、亚马逊 Kendra Amazon CodeArtifact、亚马逊 Macie、亚马逊 Route 53、亚马逊 A Amazon Transfer Family I、Amazon Pinpoint、、SageMaker Resilience Hub、亚马逊 Amazon Migration Hub Amazon 、Di Amazon rectory Service 和。 CloudWatch Amazon WAF	2023 年 4 月 13 日

更改	描述	日期
ion, macie2:GetClassificatio nExportConfiguration, macie2 :GetCustomDataIdentifier, ma cie2:GetFindingsPublication Configuration, macie2:ListCu stomDataIdentifiers, mobiletar geting:GetEmailChannel, refa ctor-spaces:GetEnvironment, refactor-spaces:ListEnviron ments, resiliencehub:ListTag sForResource, route53:G etDNSSEC, sagemaker :DescribeDomain, sagemaker :DescribeModelBiasJobDefini tion, sagemaker:Des cribeModelQualityJobDefinit ion, sagemaker:DescribePipel ine, sagemaker:Describe Project, sagemaker:ListDomai ns, sagemaker:ListMode lBiasJobDefinitions, sagemak er:ListModelQualityJobDefin itions, sagemaker:ListPipe lines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificat e, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLogging Configurations		

更改	描述	日期
AWS_ConfigRole – 添加 amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, ec2:GetInstanceTypesFromInstanceRequirement, ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfiguration, macie2:GetClassificatio	该政策现在支持亚马逊托管工作流程的额外权限，包括、、、亚马逊 Amazon Amplify、、亚马逊弹性计算云 Amazon App Mesh Amazon App Runner CloudFront、亚马逊 Kendra Amazon CodeArtifact、亚马逊 Macie、亚马逊 Route 53、亚马逊 A Amazon Transfer Family I、Amazon Pinpoint、、SageMaker Resilience Hub、亚马逊 Amazon Migration Hub Amazon 、Di Amazon rectory Service 和。 CloudWatch Amazon WAF	2023 年 4 月 13 日

更改	描述	日期
nExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudfront:GetResponseHeadersPolicy, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig, groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstancePro	该政策现在支持亚马逊、亚马逊 WorkSpaces 应用程序、亚马逊、亚马逊 AppFlow、、、、亚马逊、、 Amazon App Runner、Amazon CloudWatch Evicently CloudFront、Amazon F CloudWatch orecast Amazon CodeArtifact Amazon CodeCommit Amazon Device Farm、Amazon Identity and Access Management (IAM)、、Amazon MemoryDB Amazon IoT、Amazon Pinpoint、、、、亚马逊关系数据库 Amazon Panorama服务 (Amazon RDS) Amazon Network Manager、Amazon Redshift 和亚马逊 AI 的额外权限。 Amazon Ground Station SageMaker	2023 年 3 月 30 日

更改	描述	日期
file, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

更改	描述	日期
AWS_ConfigRole – 添加 appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundstation:GetConfig,	该政策现在支持亚马逊、亚马逊 WorkSpaces 应用程序、亚马逊、亚马逊 AppFlow、、、、 Amazon App Runner、亚马逊弹性计算云（亚马逊） Amazon CloudFormation CloudFront、亚马逊 CloudWatch Evicently CloudWatch Amazon CodeArtifact Amazon CodeCommit Amazon Device Farm、Amazon Forecast、 Amazon Identity and Access Management （IAM EC2）、、Amazon MemoryDB Amazon Ground Station、Amazon Pinpoint Amazon IoT、、、、亚马逊关系数据库 Amazon Panorama 服务（亚马逊 RDS） Amazon Network Manager、亚马逊 Redshift 和亚马逊的额外权限人工智能。 SageMaker	2023 年 3 月 30 日

更改	描述	日期
groundstation:ListConfigs, groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

更改	描述	日期
AWSConfigRulesExecutionRole— Amazon Config 开始跟踪此 Amazon 托管策略的更改	此策略允许 Amazon Lambda 函数访问定期发送到 Amazon S3 的 Amazon Config Amazon Config API 和配置快照。评估 Amazon 自定义 Lambda 规则的配置更改的函数需要此访问权限。	2023 年 3 月 7 日
AWSConfigRoleForOrganizations— Amazon Config 开始跟踪此 Amazon 托管策略的更改	此策略 Amazon Config 允许只读调用 Amazon Organizations APIs。	2023 年 3 月 7 日
AWSConfigRemediationServiceRolePolicy— Amazon Config 开始跟踪此 Amazon 托管策略的更改	此政策 Amazon Config 允许代表您修复NON_COMPLIANT 资源。	2023 年 3 月 7 日
AWSConfigServiceRolePolicy – 添加 auditmanager:GetAccountStatus	此策略现在授予返回 Amazon Audit Manager中的账户注册状态的权限。	2023 年 3 月 3 日
AWS_ConfigRole – 添加 auditmanager:GetAccountStatus	此策略现在授予返回 Amazon Audit Manager中的账户注册状态的权限。	2023 年 3 月 3 日
AWSConfigMultiAccountSetupPolicy— Amazon Config 开始跟踪此 Amazon 托管策略的更改	此策略 Amazon Config 允许使用调用 Amazon 服务并在整个组织中部署 Amazon Config 资源 Amazon Organizations。	2023 年 2 月 27 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	该政策现在支持Apache Airflow、Amazon Applications Amazon IoT、Amazon WorkSpaces Reviewer Amazon HealthLake、Ama CodeGuru zon Kinesis Video Streams、亚马逊应用程序恢复控制器 (ARC)、亚马逊弹性计算云 (亚马逊) Amazon Device Farm、亚马逊 Pinpoin Amazon Identity and Access Management t、(IAM EC2)、亚马逊和亚马逊日志的亚马逊托管工作流程的额外权限。GuardDuty CloudWatch	2023 年 2 月 1 日

更改	描述	日期
m:ListTestGridProjects，ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools，ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement，mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource，ecr:BatchGetRepositoryScanningConfiguration，iam:ListServerCertificates，guardduty:ListPublishingDestinations，guardduty:DescribePublishingDestination, logs:GetLogDelivery，and logs:ListLogDeliveries		

更改	描述	日期
AWS_ConfigRole – 添加 airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	该政策现在支持Apache Airflow、Amazon Applications Amazon IoT、Amazon WorkSpaces Reviewer Amazon HealthLake、Ama CodeGuru zon Kinesis Video Streams、亚马逊应用程序恢复控制器 (ARC)、亚马逊弹性计算云 (亚马逊) Amazon Device Farm、亚马逊 Pinpoin Amazon Identity and Access Management t、(IAM EC2)、亚马逊和亚马逊日志的亚马逊托管工作流程的额外权限。GuardDuty CloudWatch	2023 年 2 月 1 日

更改	描述	日期
m:ListTestGridProjects，ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools，ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement，mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource，ecr:BatchGetRepositoryScanningConfiguration，iam:ListServerCertificates，guardduty:ListPublishingDestinations，guardduty:DescribePublishingDestination, logs:GetLogDelivery，and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – 更新 config:DescribeConfigRules	作为安全最佳实践，此策略现在取消了对 `config:DescribeConfigRules` 的广泛资源级别权限。	2023 年 1 月 12 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, Amazon Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	该政策现在支持亚马逊托管服务 Prometheus、、、、、、、、、、、亚马逊弹性计算云 Amazon Database Migration Service（亚马逊Amazon DMS）Amazon Audit Manager Amazon Device Farm、、 Amazon Directory Service、Amazon Lightsail、、 Amazon Glue、EC2 Ama Amazon IoT zon Quick Suite、 AWS Elemental MediaPackage、 Amazon Network Manager亚马逊应用程序恢复控制器 (ARC) Amazon Resource Access Manager、亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 的额外权限。	2022 年 12 月 15 日

更改	描述	日期
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

更改	描述	日期
AWS_ConfigRole – 添加 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	该政策现在支持亚马逊托管服务 Prometheus、、、、、、、、、、亚马逊弹性计算云 Amazon Database Migration Service（亚马逊Amazon DMS）Amazon Audit Manager Amazon Device Farm、、 Amazon Directory Service、Amazon Lightsail、、 Amazon Glue、EC2 Ama Amazon IoT zon Quick Suite、 AWS Elemental MediaPackage、 Amazon Network Manager亚马逊应用程序恢复控制器 (ARC) Amazon Resource Access Manager、亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 的额外权限。	2022 年 12 月 15 日

更改	描述	日期
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 cloudformation:ListStackResources and cloudformation:ListStacks	现在，此策略允许返回指定 Amazon CloudFormation 堆栈中所有资源的描述并返回状态与指定StackStatusFilter堆栈的摘要信息。	2022 年 11 月 7 日
AWS_ConfigRole – 添加 cloudformation:ListStackResources and cloudformation:ListStacks	现在，此策略允许返回指定 Amazon CloudFormation 堆栈中所有资源的描述并返回状态与指定StackStatusFilter堆栈的摘要信息。	2022 年 11 月 7 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	该政策现在支持以下方面的额外权限：Apache Airflow Amazon Certificate Manager、、、亚马逊密钥空间 Amazon Amplify、 Amazon AppConfig亚马逊、Amazon Connect CloudWatch、亚马逊弹性计算云（亚马逊） Amazon Glue DataBrew、亚马逊弹性 Kubernetes 服务（ EC2亚马逊 EKS）、亚马逊、、亚马逊欺诈探测器、亚马逊、亚马逊服务器、亚马逊定位服务、、Amazon Lex EventBridge、 Amazon Fault Injection Service Amazon Lightsail FSx、A GameLift mazon Pinpoint Amazon IoT、、、、Amazon Quick Suite、亚马逊关系数据库 Amazon OpsWorks Amazon Panorama Amazon Resource Access Manager服务（亚马逊 RDS）、亚马逊 Amazon RoboMaker Rekognition、、、Amazon Route 53 Amazon Resource Groups、亚马逊简单存储服务 Amazon Cloud Map(Amazon S3) Simple Service 和。 Amazon Security Token Service	2022 年 10 月 19 日

更改	描述	日期
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

更改	描述	日期
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

更改	描述	日期
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

更改	描述	日期
AWS_ConfigRole – 添加 acm-pca:GetCertificateAuthorityCsr，acm-pca:ListCertificateAuthorities, acm-pca:ListTags，airflow:GetEnvironment, airflow:ListEnvironments，amplifyuibuilder:ListThemes，appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments，appconfig:ListHostedConfigurationVersions, cassandra:Select，cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard， cloudwatch:ListDashboards, connect:DescribePhoneNumber，connect:ListPhoneNumbers, connect:ListPhoneNumbersV2， connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset，databrew:DescribeJob, databrew:DescribeProject，databrew:DescribeRecipe, databrew:DescribeRuleset，databrew:DescribeSchedule, databrew:ListDatasets，databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes， databrew:ListRecipeVers	该政策现在支持以下方面的额外权限：Apache Airflow Amazon Certificate Manager、、、亚马逊密钥空间 Amazon Amplify、 Amazon AppConfig亚马逊、Amazon Connect CloudWatch、亚马逊弹性计算云（亚马逊） Amazon Glue DataBrew、亚马逊弹性 Kubernetes 服务（ EC2亚马逊 EKS）、亚马逊、、亚马逊欺诈探测器、亚马逊、亚马逊服务器、亚马逊定位服务、、Amazon Lex EventBridge、 Amazon Fault Injection Service Amazon Lightsail FSx、A GameLift mazon Pinpoint Amazon IoT、、、、Amazon Quick Suite、亚马逊关系数据库 Amazon OpsWorks Amazon Panorama Amazon Resource Access Manager服务（亚马逊 RDS）、亚马逊 Amazon RoboMaker Rekognition、、、Amazon Route 53 Amazon Resource Groups、亚马逊简单存储服务 Amazon Cloud Map(Amazon S3) Simple Service 和。 Amazon Security Token Service	2022 年 10 月 19 日

更改	描述	日期
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

更改	描述	日期
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

更改	描述	日期
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 Glue::GetTable	现在，此策略授予在数据目录中检索指定 Amazon Glue 表的表定义的权限。	2022 年 9 月 14 日
AWS_ConfigRole – 添加 Glue::GetTable	现在，此策略授予在数据目录中检索指定 Amazon Glue 表的表定义的权限。	2022 年 9 月 14 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 appconfig:ListApplications，appflow:DescribeConnectorProfiles, appsync:GetApiCache，autoscaling-plans:DescribeScalingPlanResources，autoscaling-plans:DescribeScalingPlans，autoscaling-plans:GetScalingPlanResourceForecastData，autoscaling:DescribeWarmPool，backup:DescribeFramework，backup:DescribeReportPlan，backup:ListFrameworks，backup:ListReportPlans，budgets:DescribeBudgetAction，budgets:DescribeBudgetActionsForAccount，budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget，ce:GetAnomalyMonitors，ce:GetAnomalySubscriptions，cloud9:DescribeEnvironmentMemberships，cloud9:DescribeEnvironments, cloud9:ListEnvironments，cloud9:ListTagsForResource, cloudwatch:GetMetricStream，cloudwatch:ListMetricStreams，datasync:DescribeLocationFsxWindows，devops-guru:GetResourceCollection，ds:DescribeDirectories，ec2:DescribeTrafficMirrorFilte	该政策现在支持亚马逊 AppFlow、亚马逊、亚马 CloudWatch逊 R CloudWatch UM、Amazon S CloudWatch ynthetics、Amazon Connect 客户档案、Amazon Connect 语音识别码、亚马逊 DevOps Guru、亚马逊弹性计算云（亚马逊）、Amazon Aut EC2 o Scaling EC2、亚马逊 EMR、亚马逊、亚马逊架构、亚马逊欺诈 Amazon FinSpace探测器、亚马逊 GameLift 服务器、EventBridge亚马逊互动视频服务（ EventBridge 亚马逊 IVS））Interactive Service、适用于 Apache Flink 的亚马逊托管服务、Image Builder、Amazon Lex、Amazon Lightsail、 EC2 亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble Pinp StudioAmazon oint、亚马逊快速套件、亚马逊应用程序恢复控制器 (ARC Amazon Route 53 Resolver)、亚马逊简单存储服务 (Amazon S3)、亚马逊 SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、亚马逊 Timestream、、、、、、、、	2022 年 9 月 7 日

更改	描述	日期
rs，ec2:DescribeTrafficMirrorTargets，ec2:GetNetworkInsightsAccessScopeAnalysisFindings，ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio，elasticmapreduce:GetStudioSessionMapping，elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings，events:DescribeEndpoint, events:DescribeEventBus，events:DescribeRule，events:ListArchives, events:ListEndpoints，events:ListEventBuses, events:ListRules，events:ListTagsForResource，events:ListTargetsByRule，finspace:GetEnvironment，finspace:ListEnvironments，frauddetector:GetDetectors，frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes, frauddetector:GetEventTypes，frauddetector:GetExternalModels, frauddetector:GetLabels，frauddetector:GetModels, frauddetector:GetOutcomes，frauddetector:GetVariables, frauddetector:ListTagsForResource，gamelift:DescribeAlias, gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity，	、、、、、、、、、、、、、、、、、、、、、Amazon AppConfig Amazon AppSync Amazon Auto Scaling Amazon Backup Amazon Budgets Amazon Cost Explorer Amazon Cloud9 Amazon Directory Service Amazon DataSync AWS Elemental MediaPackage Amazon Glue Amazon IoT Amazon IoT Analytics Amazon IoT Events Amazon IoT SiteWise、 Amazon IoT TwinMaker、 Amazon Lake Formation、 Amazon License Manager、 Amazon Resilience Hub、 Amazon Signer、和 Amazon Transfer Family。	

更改	描述	日期
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

更改	描述	日期
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

更改	描述	日期
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

更改	描述	日期
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

更改	描述	日期
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

更改	描述	日期
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

更改	描述	日期
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

更改	描述	日期
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

更改	描述	日期
AWS_ConfigRole – 添加 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	该政策现在支持亚马逊 AppFlow、亚马逊、亚马 CloudWatch逊 R CloudWatch UM、Amazon S CloudWatch ynthetics、Amazon Connect 客户档案、Amazon Connect 语音识别码、亚马逊 DevOps Guru、亚马逊弹性计算云（亚马逊）、Amazon Aut EC2 o Scaling EC2、亚马逊 EMR、亚马逊、亚马逊架构、亚马逊欺诈 Amazon FinSpace探测器、亚马逊 GameLift 服务器、EventBridge亚马逊互动视频服务（ EventBridge 亚马逊 IVS））Interactive Service、适用于 Apache Flink 的亚马逊托管服务、Image Builder、Amazon Lex、Amazon Lightsail、 EC2 亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble Pinp StudioAmazon oint、亚马逊快速套件、亚马逊应用程序恢复控制器 (ARC Amazon Route 53 Resolver)、亚马逊简单存储服务 (Amazon S3)、亚马逊 SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、亚马逊 Timestream、、、、、、、、	2022 年 9 月 7 日

更改	描述	日期
ts，ec2:GetNetworkInsightsAccessScopeAnalysisFindings，ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio，elasticmapreduce:GetStudioSessionMapping，elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings，events:DescribeEndpoint, events:DescribeEventBus，events:DescribeRule，events:ListArchives, events:ListEndpoints，events:ListEventBuses, events:ListRules，events:ListTagsForResource，events:ListTargetsByRule，finspace:GetEnvironment，finspace:ListEnvironments，frauddetector:GetDetectors，frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes, frauddetector:GetEventTypes，frauddetector:GetExternalModels, frauddetector:GetLabels，frauddetector:GetModels, frauddetector:GetOutcomes，frauddetector:GetVariables, frauddetector:ListTagsForResource，gamelift:DescribeAlias, gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity，gamelift:DescribeFleetLocat	、、、、、、、、、、、、、、、、、、、、、、、、、Amazon AppConfig Amazon AppSync Amazon Auto Scaling Amazon Backup Amazon Budgets Amazon Cost Explorer Amazon Cloud9 Amazon Directory Service Amazon DataSync AWS Elemental MediaPackage Amazon Glue Amazon IoT Amazon IoT Analytics Amazon IoT Events Amazon IoT SiteWise、 Amazon IoT TwinMaker、 Amazon Lake Formation、 Amazon License Manager、 Amazon Resilience Hub、 Amazon Signer、和 Amazon Transfer Family	

更改	描述	日期
ionAttributes, gamelift:Des cribeFleetLocationCapacity, gamelift:DescribeFleetPort Settings, gamelift:Describe GameServerGroup, g amelift:DescribeGameSession Queues, gamelift:DescribeMa tchmakingConfigurations, ga melift:DescribeMatchmakingR uleSets, gamelift:DescribeR untimeConfiguration, gamelift: DescribeScript, gamelift:De scribeVpcPeeringAuthorizati ons, gamelift:ListAliases, gamelift:ListBuilds, gamelift: ListFleets, gamelift:ListGa meServerGroups, gamelift: ListScripts, gamelift:ListT agsForResource, geo:ListM aps, glue:GetClassifier, glue:GetClassifiers, imagebuil der:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeli ne, imagebuilder:GetImageRe cipe, imagebuilder:ListC ontainerRecipes, imagebuild er:ListImageBuildVersions, imagebuilder:ListImagePipel ines, imagebuilder:ListI mageRecipes, imagebuilder:L istImages, iot:DescribeCertif icate, iot:DescribeDimensio n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

更改	描述	日期
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

更改	描述	日期
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

更改	描述	日期
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

更改	描述	日期
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

更改	描述	日期
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

更改	描述	日期
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

更改	描述	日期
ansfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject,	该政策现在支持Apache Airflow、Amazon Applications Amazon IoT、Amazon WorkSpaces Reviewer Amazon HealthLake、Ama CodeGuru zon Kinesis Video Streams、亚马逊应用程序恢复控制器 (ARC)、亚马逊弹性计算云 (亚马逊) Amazon Device Farm、亚马逊 Pinpoin Amazon Identity and Access Management t、(IAM EC2)、亚马逊和亚马逊日志的亚马逊托管工作流程的额外权限。GuardDuty CloudWatch	2023 年 2 月 1 日

更改	描述	日期
devicefarm:ListTestGridProjects, ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools, ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings, mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

更改	描述	日期
AWS_ConfigRole – 添加 airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs, appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore, healthlake:ListTagsForResource, kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream, kinesisvideo:DescribeSignalingChannel, kinesisvideo:ListTagsForResource, kinesisvideo:ListSignalingChannels, route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters, route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules, devicefarm:GetTestGridProject, devicefar	该政策现在支持Apache Airflow、Amazon Applications Amazon IoT、Amazon WorkSpaces Reviewer Amazon HealthLake、Ama CodeGuru zon Kinesis Video Streams、亚马逊应用程序恢复控制器 (ARC)、亚马逊弹性计算云 (亚马逊) Amazon Device Farm、亚马逊 Pinpoin Amazon Identity and Access Management t、(IAM EC2)、亚马逊和亚马逊日志的亚马逊托管工作流程的额外权限。GuardDuty CloudWatch	2023 年 2 月 1 日

更改	描述	日期
m:ListTestGridProjects，ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools，ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement，mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource，ecr:BatchGetRepositoryScanningConfiguration，iam:ListServerCertificates，guardduty:ListPublishingDestinations，guardduty:DescribePublishingDestination, logs:GetLogDelivery，and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – 更新 config:DescribeConfigRules	作为安全最佳实践，此策略现在取消了对 `config:DescribeConfigRules` 的广泛资源级别权限。	2023 年 1 月 12 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, Amazon Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	该政策现在支持亚马逊托管服务 Prometheus、、、、、、、、、、亚马逊弹性计算云 Amazon Database Migration Service（亚马逊Amazon DMS）Amazon Audit Manager Amazon Device Farm、、 Amazon Directory Service、Amazon Lightsail、、 Amazon Glue、EC2 Ama Amazon IoT zon Quick Suite、 AWS Elemental MediaPackage、 Amazon Network Manager亚马逊应用程序恢复控制器 (ARC) Amazon Resource Access Manager、亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 的额外权限。	2022 年 12 月 15 日

更改	描述	日期
ions, networkmanager:ListTagsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

更改	描述	日期
AWS_ConfigRole – 添加 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTa	该政策现在支持亚马逊托管服务 Prometheus、、、、、、、、、、亚马逊弹性计算云 Amazon Database Migration Service（亚马逊Amazon DMS）Amazon Audit Manager Amazon Device Farm、、 Amazon Directory Service、Amazon Lightsail、、 Amazon Glue、EC2 Ama Amazon IoT zon Quick Suite、 AWS Elemental MediaPackage、 Amazon Network Manager亚马逊应用程序恢复控制器 (ARC) Amazon Resource Access Manager、亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 的额外权限。	2022 年 12 月 15 日

更改	描述	日期
gsForResource, quicksight:DescribeDashboard, quicksight:DescribeDashboardPermissions, quicksight:DescribeTemplate, quicksight:DescribeTemplatePermissions, quicksight:ListDashboards, quicksight:ListTemplates, ram:ListResources, route53-recovery-control-config:DescribeControlPanel, route53-recovery-control-config:ListControlPanels, route53-recovery-control-config:ListTagsForResource, route53resolver:GetResolverQueryLogConfigAssociation, route53resolver:ListResolverQueryLogConfigAssociations, s3:GetAccessPointForObjectLambda, s3:GetAccessPointPolicyForObjectLambda, s3:GetAccessPointPolicyStatusForObjectLambda, s3:GetMultiRegionAccessPoint, s3:ListAccessPointsForObjectLambda, s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints, transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 cloudformation:ListStackResources and cloudformation:ListStacks	现在，此策略允许返回指定 Amazon CloudFormation 堆栈中所有资源的描述并返回状态与指定StackStatusFilter堆栈的摘要信息。	2022 年 11 月 7 日
AWS_ConfigRole – 添加 cloudformation:ListStackResources and cloudformation:ListStacks	现在，此策略允许返回指定 Amazon CloudFormation 堆栈中所有资源的描述并返回状态与指定StackStatusFilter堆栈的摘要信息。	2022 年 11 月 7 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	该政策现在支持以下方面的额外权限：Apache Airflow Amazon Certificate Manager、、、亚马逊密钥空间 Amazon Amplify、 Amazon AppConfig亚马逊、Amazon Connect CloudWatch、亚马逊弹性计算云（亚马逊） Amazon Glue DataBrew、亚马逊弹性 Kubernetes 服务（ EC2亚马逊 EKS）、亚马逊、、亚马逊欺诈探测器、亚马逊、亚马逊服务器、亚马逊定位服务、、Amazon Lex EventBridge、 Amazon Fault Injection Service Amazon Lightsail FSx、A GameLift mazon Pinpoint Amazon IoT、、、、Amazon Quick Suite、亚马逊关系数据库 Amazon OpsWorks Amazon Panorama Amazon Resource Access Manager服务（亚马逊 RDS）、亚马逊 Amazon RoboMaker Rekognition、、、Amazon Route 53 Amazon Resource Groups、亚马逊简单存储服务 Amazon Cloud Map(Amazon S3) Simple Service 和。 Amazon Security Token Service	2022 年 10 月 19 日

更改	描述	日期
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

更改	描述	日期
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

更改	描述	日期
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

更改	描述	日期
AWS_ConfigRole – 添加 acm-pca:GetCertificateAuthorityCsr, acm-pca:ListCertificateAuthorities, acm-pca:ListTags, airflow:GetEnvironment, airflow:ListEnvironments, amplifyuibuilder:ListThemes, appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments, appconfig:ListHostedConfigurationVersions, cassandra:Select, cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber, connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset, databrew:DescribeJob, databrew:DescribeProject, databrew:DescribeRecipe, databrew:DescribeRuleset, databrew:DescribeSchedule, databrew:ListDatasets, databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	该政策现在支持以下方面的额外权限：Apache Airflow Amazon Certificate Manager、、、亚马逊密钥空间 Amazon Amplify、 Amazon AppConfig亚马逊、Amazon Connect CloudWatch、亚马逊弹性计算云（亚马逊） Amazon Glue DataBrew、亚马逊弹性 Kubernetes 服务（ EC2亚马逊 EKS）、亚马逊、、亚马逊欺诈探测器、亚马逊、亚马逊服务器、亚马逊定位服务、、Amazon Lex EventBridge、 Amazon Fault Injection Service Amazon Lightsail FSx、A GameLift mazon Pinpoint Amazon IoT、、、、Amazon Quick Suite、亚马逊关系数据库 Amazon OpsWorks Amazon Panorama Amazon Resource Access Manager服务（亚马逊 RDS）、亚马逊 Amazon RoboMaker Rekognition、、、Amazon Route 53 Amazon Resource Groups、亚马逊简单存储服务 Amazon Cloud Map(Amazon S3) Simple Service 和。 Amazon Security Token Service	2022 年 10 月 19 日

更改	描述	日期
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

更改	描述	日期
se:DescribeProject, iotsitewise:ListAssetModels, iotsitewise:ListDashboards, iotsitewise:ListGateways, iotsitewise:ListPortals, iotsitewise:ListProjectAssets, iotsitewise:ListProjects, iotsitewise:ListTagsForResource, iotwireless:GetServiceProfile, iotwireless:GetWirelessDevice, iotwireless:GetWirelessGatewayTaskDefinition, iotwireless:ListServiceProfiles, iotwireless:ListTagsForResource, iotwireless:ListWirelessDevices, iotwireless:ListWirelessGatewayTaskDefinitions, lex:DescribeBotVersion, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDatabase, lightsail:GetRelationalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign, mobiletargeting:GetSegment, mobiletargeting:GetSegments, opsworks:DescribeInstances, opsworks:DescribeTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplicationInstance, panorama:DescribeApplicationInstanceDetails,		

更改	描述	日期
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 Glue::GetTable	现在，此策略授予在数据目录中检索指定 Amazon Glue 表的表定义的权限。	2022 年 9 月 14 日
AWS_ConfigRole – 添加 Glue::GetTable	现在，此策略授予在数据目录中检索指定 Amazon Glue 表的表定义的权限。	2022 年 9 月 14 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 appconfig:ListApplications，appflow:DescribeConnectorProfiles, appsync:GetApiCache，autoscaling-plans:DescribeScalingPlanResources，autoscaling-plans:DescribeScalingPlans，autoscaling-plans:GetScalingPlanResourceForecastData，autoscaling:DescribeWarmPool，backup:DescribeFramework，backup:DescribeReportPlan，backup:ListFrameworks，backup:ListReportPlans，budgets:DescribeBudgetAction，budgets:DescribeBudgetActionsForAccount，budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget，ce:GetAnomalyMonitors，ce:GetAnomalySubscriptions，cloud9:DescribeEnvironmentMemberships，cloud9:DescribeEnvironments, cloud9:ListEnvironments，cloud9:ListTagsForResource, cloudwatch:GetMetricStream，cloudwatch:ListMetricStreams，datasync:DescribeLocationFsxWindows，devops-guru:GetResourceCollection，ds:DescribeDirectories，ec2:DescribeTrafficMirrorFilte	该政策现在支持亚马逊 AppFlow、亚马逊、亚马 CloudWatch逊 R CloudWatch UM、Amazon S CloudWatch ynthetics、Amazon Connect 客户档案、Amazon Connect 语音识别码、亚马逊 DevOps Guru、亚马逊弹性计算云（亚马逊）、Amazon Aut EC2 o Scaling EC2、亚马逊 EMR、亚马逊 EMR、亚马逊 Fraud Detector、亚马逊 GameLift 服务器、亚马逊交互式视频服务 (EventBridge亚马逊 IVS) 的额外权限) Interactive Servic EventBridge e、适用于 Apache Flink 的亚马逊托管服务、Image Builder、Amazon Lex、Amazon Lightsail、Amazon FinSpace EC2 亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble Pinp StudioAmazon oint、亚马逊快速套件、亚马逊应用程序恢复控制器 (ARC Amazon Route 53 Resolver)、亚马逊简单存储服务 (Amazon S3)、亚马逊 SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、亚马逊 Timestream、、、、、、、、	2022 年 9 月 7 日

更改	描述	日期
rs，ec2:DescribeTrafficMirrorTargets，ec2:GetNetworkInsightsAccessScopeAnalysisFindings，ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio，elasticmapreduce:GetStudioSessionMapping，elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings，events:DescribeEndpoint, events:DescribeEventBus，events:DescribeRule，events:ListArchives, events:ListEndpoints，events:ListEventBuses, events:ListRules，events:ListTagsForResource，events:ListTargetsByRule，finspace:GetEnvironment，finspace:ListEnvironments，frauddetector:GetDetectors，frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes, frauddetector:GetEventTypes，frauddetector:GetExternalModels, frauddetector:GetLabels，frauddetector:GetModels, frauddetector:GetOutcomes，frauddetector:GetVariables, frauddetector:ListTagsForResource，gamelift:DescribeAlias, gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity，	、、、、、、、、、、、、、、、、、、、、、、、、、Amazon AppConfig Amazon AppSync Amazon Auto Scaling Amazon Backup Amazon Budgets Amazon Cost Explorer Amazon Cloud9 Amazon Directory Service Amazon DataSync AWS Elemental MediaPackage Amazon Glue Amazon IoT Amazon IoT Analytics Amazon IoT Events Amazon IoT SiteWise、 Amazon IoT TwinMaker、 Amazon Lake Formation、 Amazon License Manager、 Amazon Resilience Hub、 Amazon Signer、和 Amazon Transfer Family。	

更改	描述	日期
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

更改	描述	日期
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

更改	描述	日期
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBu		

更改	描述	日期
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

更改	描述	日期
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

更改	描述	日期
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

更改	描述	日期
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

更改	描述	日期
transfer:DescribeServer, transfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

更改	描述	日期
AWS_ConfigRole – 添加 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	该政策现在支持亚马逊 AppFlow、亚马逊、亚马 CloudWatch逊 R CloudWatch UM、Amazon S CloudWatch ynthetics、Amazon Connect 客户档案、Amazon Connect 语音识别码、亚马逊 DevOps Guru、亚马逊弹性计算云（亚马逊）、Amazon Aut EC2 o Scaling EC2、亚马逊 EMR、亚马逊 EMR、亚马逊 Fraud Detector、亚马逊 GameLift 服务器、亚马逊交互式视频服务 (EventBridge亚马逊 IVS) 的额外权限) Interactive Servic EventBridge e、适用于 Apache Flink 的亚马逊托管服务、Image Builder、Amazon Lex、Amazon Lightsail、Amazon FinSpace EC2 亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble Pinp StudioAmazon oint、亚马逊快速套件、亚马逊应用程序恢复控制器 (ARC Amazon Route 53 Resolver)、亚马逊简单存储服务 (Amazon S3)、亚马逊 SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、亚马逊 Timestream、、、、、、、、	2022 年 9 月 7 日

更改	描述	日期
ts，ec2:GetNetworkInsightsAccessScopeAnalysisFindings，ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio，elasticmapreduce:GetStudioSessionMapping，elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings，events:DescribeEndpoint, events:DescribeEventBus，events:DescribeRule，events:ListArchives, events:ListEndpoints，events:ListEventBuses, events:ListRules，events:ListTagsForResource，events:ListTargetsByRule，finspace:GetEnvironment，finspace:ListEnvironments，frauddetector:GetDetectors，frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes, frauddetector:GetEventTypes，frauddetector:GetExternalModels, frauddetector:GetLabels，frauddetector:GetModels, frauddetector:GetOutcomes，frauddetector:GetVariables, frauddetector:ListTagsForResource，gamelift:DescribeAlias, gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity，gamelift:DescribeFleetLocat	、、、、、、、、、、、、、、、、、、、、、Amazon AppConfig Amazon AppSync Amazon Auto Scaling Amazon Backup Amazon Budgets Amazon Cost Explorer Amazon Cloud9 Amazon Directory Service Amazon DataSync AWS Elemental MediaPackage Amazon Glue Amazon IoT Amazon IoT Analytics Amazon IoT Events Amazon IoT SiteWise、 Amazon IoT TwinMaker、 Amazon Lake Formation、 Amazon License Manager、 Amazon Resilience Hub、 Amazon Signer、和 Amazon Transfer Family	

更改	描述	日期
ionAttributes, gamelift:Des cribeFleetLocationCapacity, gamelift:DescribeFleetPort Settings, gamelift:Describe GameServerGroup, g amelift:DescribeGameSession Queues, gamelift:DescribeMa tchmakingConfigurations, ga melift:DescribeMatchmakingR uleSets, gamelift:DescribeR untimeConfiguration, gamelift: DescribeScript, gamelift:De scribeVpcPeeringAuthorizati ons, gamelift:ListAliases, gamelift:ListBuilds, gamelift: ListFleets, gamelift:ListGa meServerGroups, gamelift: ListScripts, gamelift:ListT agsForResource, geo:ListM aps, glue:GetClassifier, glue:GetClassifiers, imagebuil der:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeli ne, imagebuilder:GetImageRe cipe, imagebuilder:ListC ontainerRecipes, imagebuild er:ListImageBuildVersions, imagebuilder:ListImagePipel ines, imagebuilder:ListI mageRecipes, imagebuilder:L istImages, iot:DescribeCertif icate, iot:DescribeDimensio n, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

更改	描述	日期
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

更改	描述	日期
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

更改	描述	日期
lightsail:GetDisk, lightsail :GetDisks, lightsail:GetInsta nce, lightsail:GetInstances , lightsail:GetKeyPair, light sail:GetLoadBalancer, lightsail :GetLoadBalancers, lightsai l:GetLoadBalancerTlsCertifi cates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookout equipment:DescribeInference Scheduler, lookoutequipment :ListTagsForResource, looko utmetrics:DescribeAlert, lo okoutmetrics:DescribeAnomal yDetector, lookoutmetrics:L istAlerts, lookoutmetrics:Lis tAnomalyDetectors, lookoutm etrics:ListMetricSets, look outmetrics:ListTagsForResou rce, lookoutvision:Describe Project, lookoutvision:List Projects, managedblockchain :GetMember, managedbl ockchain:GetNetwork, managedblockchain:GetNod e, managedblockchain:ListInvit ations, managedblockchain:L istMembers, managedbl ockchain:ListNodes, mediapa ckage-vod:DescribePackaging Group, mediapackage- vod:ListPackagingGroups, mediapackage-vod:ListTagsFo rResource, mobiletargeting: GetInAppTemplate, mobiletar		

更改	描述	日期
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

更改	描述	日期
olicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint, s3-outposts:GetAccessPoint		

更改	描述	日期
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

更改	描述	日期
ansfer:DescribeUser, transfer: DescribeWorkflow, transfer: ListServers, transfer:ListUsers , transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy – 添加 datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	此策略现在允许返回中 Amazon DataSync 代理人、DataSync 来源和目标位置以及 DataSync 任务的列表 Amazon Web Services 账户；列出与中一个或多个指定命名空间关联的 Amazon Cloud Map 命名空间和服务的摘要信息 Amazon Web Services 账户；以及列出中所有可用的 Amazon Simple Email Service (Amazon SES) 联系人列表。 Amazon Web Services 账户	2022 年 8 月 22 日
AWS_ConfigRole – 添加 datasync:ListAgents, datasync:ListLocations, dat async:ListTasks, servicedi scovery:ListNamespaces, ser vicediscovery:ListServices, and ses:ListContactLists	此策略现在允许返回中 Amazon DataSync 代理人、DataSync 来源和目标位置以及 DataSync 任务的列表 Amazon Web Services 账户；列出与中一个或多个指定命名空间关联的 Amazon Cloud Map 命名空间和服务的摘要信息 Amazon Web Services 账户；以及列出中所有可用的 Amazon Simple Email Service (Amazon SES) 联系人列表。 Amazon Web Services 账户	2022 年 8 月 22 日

更改	描述	日期
ConfigConformsServiceRolePolicy – 添加 cloudwatch:PutMetricData	该政策现在授予向 Amazon 发布指标数据点的权限 CloudWatch。	2022 年 7 月 25 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	该政策现在支持亚马逊弹性容器服务 (Amazon ECS)、亚马逊、亚马逊、亚马逊、亚马逊、适用于 A ElastiCache pache Flink 的亚马逊托管服务 FSx、亚马逊定位服务、适用于 Apache Kafka 的亚马逊托管流媒体、亚马逊 Quick Suite、亚马逊 Rekognition、亚马逊简单存储服务 (Amazon S3) 的额外权限 Service、Amazon RoboMaker亚马逊简单电子邮件服务 (Amazon SES)、、、、、、、、、、（IAM 身份中心）Amazon Amplify Amazon DataSync、Amazon Firewall Manager Image Bu Amazon AppConfig il Amazon AppSync der 和 Elastic Load EventBridge Amazon Billing Conductor Amazon Glue Amazon IAM Identity Center EC2 平衡。	2022 年 7 月 15 日

更改	描述	日期
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

更改	描述	日期
ions, imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

更改	描述	日期
sso:GetInlinePolicyForPermissionSet		

更改	描述	日期
AWS_ConfigRole – 添加 amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	该政策现在支持亚马逊弹性容器服务 (Amazon ECS)、亚马逊、亚马逊、亚马逊、亚马逊、适用于 A ElastiCache pache Flink 的亚马逊托管服务 FSx、亚马逊定位服务、适用于 Apache Kafka 的亚马逊托管流媒体、亚马逊 Quick Suite、亚马逊 Rekognition、亚马逊简单存储服务 (Amazon S3) 的额外权限 Service、Amazon RoboMaker亚马逊简单电子邮件服务 (Amazon SES)、、、、、、、、、、（IAM 身份中心）Amazon Amplify Amazon DataSync、Amazon Firewall Manager Image Bu Amazon AppConfig il Amazon AppSync der 和 Elastic Load EventBridge Amazon Billing Conductor Amazon Glue Amazon IAM Identity Center EC2 平衡。	2022 年 7 月 15 日

更改	描述	日期
scribeLocationS3, datasync: DescribeLocationSmb, datasync:DescribeTask, datasync: ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVersions, imagebuilder: ListCompo		

更改	描述	日期
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

更改	描述	日期
sso:GetInlinePolicyForPermissionSet		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	此政策现在授予以下权限：获取指定的 Amazon Athena 数据目录 Amazon Web Services 账户、在中列出 Athena 数据目录以及列出与 Athena 工作组或数据目录资源关联的标签；获取 Amazon Detective 行为图列表并列出侦探行为图的标签；获取给定开发终端节点名称列表的资源元数据列表，获取有关指定开发的信息端点，获取所有开发端点，检索 Amazon Glue 指定的安全 Amazon Glue Amazon Glue Amazon Web Services 账户 Amazon Glue 配置，获取所有 Amazon Glue 安全配置，获取与 Amazon Glue 资源关联的标签列表，获取有关具有指定名称 Amazon Glue 的工作组的信息，检索 Amazon 账户中所有 Amazon Glue 爬虫资源的名称，获取中所有 Amazon Glue `DevEndpoint` 资源的名称，列出中所有 Amazon Glue 作业资源的名称 Amazon Web Services 账户，获取 Amazon Glue 成员账户的详细信息，列出账户中创建 Amazon Glue 的工作流名称，以及列出账户中可用 Amazon Glue 的工作组； Amazon Web Services 账户检索有关 Amazon GuardDuty 筛选器的	2022 年 5 月 31 日

更改	描述	日期
scribePermissionSet，sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets，and sso:ListTagsForResource	详细信息 GuardDuty IPSet、检索 GuardDutyThreatIntelSet、检索、检索 GuardDuty 成员账户、获取 GuardDuty筛选条件列表、获取 GuardDuty 服务、检索GuardDuty 服务标签并获取服务的信息；获取 Amazon Macie 账户的当前状态和配置设置；检索 Amazon Resource Access Manager (Amazon RAM) 资源共享的资源和委托人关联以及检索有关资源的详细信息 IPSets ThreatIntelSets GuardDuty Amazon RAM 共享；要获取有关亚马逊简单电子邮件服务 (Amazon SES) 现有配置集的信息，请获取与 Amazon SES 配置集关联的事件目标列表，并列出与 Amazon SES 账户关联的所有配置集；要获取身份中心目录属性列表，请获取权限集的详细信息，获取附加到指定 IAM 身份中心的 IAM 托管策略设置，获取为 IAM 身份中心实例设置的权限，并获取 IAM 身份的标签 Amazon IAM Identity Center 中心资源。	

更改	描述	日期
AWS_ConfigRole – 添加 athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	此政策现在授予以下权限：获取指定的 Amazon Athena 数据目录 Amazon Web Services 账户、在中列出 Athena 数据目录以及列出与 Athena 工作组或数据目录资源关联的标签；获取 Amazon Detective 行为图列表并列出侦探行为图的标签；获取给定开发终端节点名称列表的资源元数据列表，获取有关指定开发的信息端点，获取所有开发端点，检索 Amazon Glue 指定的安全 Amazon Glue Amazon Glue Amazon Web Services 账户 Amazon Glue 配置，获取所有 Amazon Glue 安全配置，获取与 Amazon Glue 资源关联的标签列表，获取有关具有指定名称 Amazon Glue 的工作组的信息，检索 Amazon 账户中所有 Amazon Glue 爬虫资源的名称，获取中所有 Amazon Glue `DevEndpoint` 资源的名称，列出中所有 Amazon Glue 作业资源的名称 Amazon Web Services 账户，获取 Amazon Glue 成员账户的详细信息，列出账户中创建 Amazon Glue 的工作流名称，以及列出账户中可用 Amazon Glue 的工作组； Amazon Web Services 账户检索有关 Amazon GuardDuty 筛选器的	2022 年 5 月 31 日

更改	描述	日期
scribePermissionSet，sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets，and sso:ListTagsForResource	详细信息 GuardDuty IPSet、检索 GuardDutyThreatIntelSet、检索、检索 GuardDuty 成员账户、获取 GuardDuty筛选条件列表、获取 GuardDuty 服务、检索GuardDuty 服务标签并获取服务的信息；获取 Amazon Macie 账户的当前状态和配置设置；检索 Amazon Resource Access Manager (Amazon RAM) 资源共享的资源和委托人关联以及检索有关资源的详细信息 IPSets ThreatIntelSets GuardDuty Amazon RAM 共享；要获取有关亚马逊简单电子邮件服务 (Amazon SES) 现有配置集的信息，请获取与 Amazon SES 配置集关联的事件目标列表，并列出与 Amazon SES 账户关联的所有配置集；要获取身份中心目录属性列表，请获取权限集的详细信息，获取附加到指定 IAM 身份中心的 IAM 托管策略设置，获取为 IAM 身份中心实例设置的权限，并获取 IAM 身份的标签 Amazon IAM Identity Center 中心资源。	

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	此策略现在授予以下权限：获取有关所有或指定 Amazon CloudTrail 事件数据存储 (EDS) 的信息、获取有关全部或指定 Amazon CloudFormation 资源的信息、获取 DynamoDB 加速器 (DAX) 参数组或子网组的列表、获取 Amazon Database Migration Service 有关当前正在访问的区域中您的账户的Amazon DMS() 复制任务的信息，以及获取指定类型的所有策略的列表。 Amazon Organizations	2022 年 4 月 7 日
AWS_ConfigRole – 添加 cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	此策略现在授予以下权限：获取有关所有或指定 Amazon CloudTrail 事件数据存储 (EDS) 的信息、获取有关全部或指定 Amazon CloudFormation 资源的信息、获取 DynamoDB 加速器 (DAX) 参数组或子网组的列表、获取 Amazon Database Migration Service 有关当前正在访问的区域中您的账户的Amazon DMS() 复制任务的信息，以及获取指定类型的所有策略的列表。 Amazon Organizations	2022 年 4 月 7 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	该策略现在支持、、DynamoDB 加速器 Amazon Backup Amazon Batch、亚马逊 DynamoDB、 Amazon Database Migration Service 亚马逊弹性计算云（ EC2 亚马逊）、亚马逊 Elastic Kubernetes Service、亚马逊、、、、亚马逊关系数据库服务、V2 和 FSx亚马逊的额外权限。 GuardDuty Amazon Key Management Service Amazon OpsWorks Amazon WAF WorkSpaces	2022 年 3 月 14 日

更改	描述	日期
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

更改	描述	日期
AWS_ConfigRole – 添加 backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	该策略现在支持、、DynamoDB 加速器 Amazon Backup Amazon Batch、亚马逊 DynamoDB、 Amazon Database Migration Service 亚马逊弹性计算云（ EC2 亚马逊）、亚马逊 Elastic Kubernetes Service、亚马逊、、、、亚马逊关系数据库服务、V2 和 FSx亚马逊的额外权限。 GuardDuty Amazon Key Management Service Amazon OpsWorks Amazon WAF WorkSpaces	2022 年 3 月 14 日

更改	描述	日期
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		
AWSConfigServiceRolePolicy – 添加 elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	现在，该策略允许获取有关 Elastic Beanstalk 环境的详细信息以及指定 Elastic Beanstalk 配置集的设置描述、获取或 Elasticsearch 版本 OpenSearch 的地图、描述数据库可用的 Amazon RDS 选项组以及获取有关部署配置的信息。 CodeDeploy 该策略现在还授予以下权限：检索附加到的指定备用联系人 Amazon Web Services 账户、检索有关 Amazon Organizations 策略的信息、检索 Amazon ECR 存储库策略、检索有关存档 Amazon Config 规则的信息、检索 Amazon ECS 任务定义系列列表、列出指定子 OU 或账户的根或上级组织单位 (OUs)，以及列出附加到指定目标根目录、组织单位或账户的策略。	2022 年 2 月 10 日

更改	描述	日期
AWS_ConfigRole – 添加 elasticbeanstalk:DescribeEnvironments，elasticbeanstalk:DescribeConfigurationSettings，account:GetAlternateContact, organizations:DescribePolicy，organizations:ListParents, organizations:ListPoliciesForTarget，es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups，rds:DescribeOptionGroups, es:GetCompatibleVersions，codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy，access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	现在，该策略允许获取有关 Elastic Beanstalk 环境的详细信息以及指定 Elastic Beanstalk 配置集的设置描述、获取或 Elasticsearch 版本 OpenSearch 的地图、描述数据库可用的 Amazon RDS 选项组以及获取有关部署配置的信息。 CodeDeploy 该策略现在还授予以下权限：检索附加到的指定备用联系人 Amazon Web Services 账户、检索有关 Amazon Organizations 策略的信息、检索 Amazon ECR 存储库策略、检索有关存档 Amazon Config 规则的信息、检索 Amazon ECS 任务定义系列列表、列出指定子 OU 或账户的根或上级组织单位 (OUs)，以及列出附加到指定目标根目录、组织单位或账户的策略。	2022 年 2 月 10 日
AWSConfigServiceRolePolicy – 添加 logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	该策略现在授予创建 Amazon CloudWatch 日志组和流以及向已创建的日志流写入日志的权限。	2021 年 12 月 15 日
AWS_ConfigRole – 添加 logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	该策略现在授予创建 Amazon CloudWatch 日志组和流以及向已创建的日志流写入日志的权限。	2021 年 12 月 15 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	该策略现在授予获取有关亚马逊 OpenSearch 服务（OpenSearch 服务）的详细信息 domain/domains 以及获取特定亚马逊关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表的权限。该政策还授予获取有关Ama ElastiCache zon快照的详细信息的权限。	2021 年 9 月 8 日
AWS_ConfigRole – 添加 es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	该策略现在授予获取有关亚马逊 OpenSearch 服务（OpenSearch 服务）的详细信息 domain/domains 以及获取特定亚马逊关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表的权限。该政策还授予获取有关Ama ElastiCache zon快照的详细信息的权限。	2021 年 9 月 8 日

更改	描述	日期
AWSConfigServiceRolePolicy— 添加logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine Amazon 资源类型以及其他权限	此策略现在授予列出日志组的标签，列出状态机的标签，以及列出所有状态机的权限。此策略现在授予获取有关状态机的详细信息的权限。该政策现在还支持亚马逊 EC2 系统管理器 (SSM)、亚马逊弹性容器注册表、亚马逊、亚马逊数据 Firehose FSx、亚马逊管理流媒体 Kafka（亚马逊 MSK）、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Route 53、亚马逊 AI SageMaker 、亚马逊简单通知服务、和。 Amazon Database Migration Service Amazon Global Accelerator Amazon Storage Gateway	2021 年 7 月 28 日

更改	描述	日期
AWS_ConfigRole— 添加 logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine 以及 Amazon 资源类型的其他权限	此策略现在授予列出日志组的标签，列出状态机的标签，以及列出所有状态机的权限。此策略现在授予获取有关状态机的详细信息的权限。该政策现在还支持亚马逊 EC2 系统管理器 (SSM)、亚马逊弹性容器注册表、亚马逊、亚马逊数据 Firehose FSx、亚马逊管理流媒体 Kafka（亚马逊 MSK）、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Route 53、亚马逊 AI SageMaker 、亚马逊简单通知服务、和。 Amazon Database Migration Service Amazon Global Accelerator Amazon Storage Gateway	2021 年 7 月 28 日

更改	描述	日期
AWSConfigServiceRolePolicy— 为 Amazon 资源类型添加ssm:DescribeDocumentPermission权限和其他权限	此策略现在授予查看有关 IAM Access Analyzer 的 Amazon Systems Manager 文档和信息的权限。该政策现在支持亚马逊 Kinesis、亚马逊、亚马逊 EMR、 ElastiCache亚马逊 Route 53 和 Amazon Network Firewall亚马逊关系数据库服务 (Amazon RDS) 的其他 Amazon 资源类型。这些权限更改 Amazon Config 允许调用支持这些资源类型APIs所需的只读权限。此策略现在还支持筛选lambda-inside-vpc Amazon Config 托管规则的 Lambda @Edge 函数。	2021 年 6 月 8 日
AWS_ConfigRole— 为 Amazon 资源类型添加 ssm:DescribeDocumentPermission权限和其他权限	此策略现在授予查看有关 IAM Access Analyzer 的 Amazon Systems Manager 文档和信息的权限。该政策现在支持亚马逊 Kinesis、亚马逊、亚马逊 EMR、 ElastiCache亚马逊 Route 53 和 Amazon Network Firewall亚马逊关系数据库服务 (Amazon RDS) 的其他 Amazon 资源类型。这些权限更改 Amazon Config 允许调用支持这些资源类型APIs所需的只读权限。此策略现在还支持筛选lambda-inside-vpc Amazon Config 托管规则的 Lambda @Edge 函数。	2021 年 6 月 8 日

更改	描述	日期
AWSConfigServiceRolePolicy— 添加apigateway:GET对 API Gateway 进行只读 GET 调用的s3:GetAccessPointPolicys3:GetAccessPointPolicyStatus权限以及只读调用 Amazon S3 的权限和权限 APIs	现在，此策略授予 Amazon Config 允许对 API Gateway 进行只读 GET 调用的权限，以支持 API 网关的 Amazon Config 规则。该策略还增加了允许 Amazon Config 以 APIs 只读方式调用 Amazon Simple Storage Service (Amazon S3) 的权限，这些权限是支持`AWS::S3::AccessPoint` 新资源类型所必需的。	2021 年 5 月 10 日
AWS_ConfiGrole — 添加apigateway:GET对 API Gateway 进行只读 GET 调用的s3:GetAccessPointPolicy权限以及只读调用 Amazon S3 的s3:GetAccessPointPolicyStatus权限和权限 APIs	现在，此策略授予的权限 Amazon Config 允许对 API Gateway 进行只读 GET 调用， Amazon Config 以支持 API 网关。该策略还增加了允许 Amazon Config 以 APIs只读方式调用 Amazon Simple Storage Service (Amazon S3) 的权限，这些权限是支持`AWS::S3::AccessPoint` 新资源类型所必需的。	2021 年 5 月 10 日

更改	描述	日期
AWSConfigServiceRolePolicy— 为 Amazon 资源类型添加ssm:ListDocuments权限和其他权限	此策略现在授予查看有关 Amazon Systems Manager 指定文档信息的权限 该政策现在还支持亚马逊弹性文件系统 Amazon Backup、亚马逊、亚马逊简单存储服务 (Amazon S3) ElastiCache、亚马逊弹性计算云 (亚马逊)、Amazon Kinesis、Amazon AI 和 EC2 亚马逊 SageMaker Route 53 的其他 Amazon 资源类型。Amazon Database Migration Service这些权限更改 Amazon Config 允许调用支持这些资源类型 APIs 所需的只读权限。	2021 年 4 月 1 日
AWS_ConfigRole— 为 Amazon 资源类型添加ssm:ListDocuments权限和其他权限	此策略现在授予查看有关 Amazon Systems Manager 指定文档信息的权限 该政策现在还支持亚马逊弹性文件系统 Amazon Backup、亚马逊、亚马逊简单存储服务 (Amazon S3) ElastiCache、亚马逊弹性计算云 (亚马逊)、Amazon Kinesis、Amazon AI 和 EC2 亚马逊 SageMaker Route 53 的其他 Amazon 资源类型。Amazon Database Migration Service这些权限更改 Amazon Config 允许调用支持这些资源类型 APIs 所需的只读权限。	2021 年 4 月 1 日
AWSConfigRole 已弃用	AWSConfigRole 已弃用。替换策略是。AWS_ConfigRole	2021 年 4 月 1 日

更改	描述	日期
Amazon Config 已开始跟踪更改	Amazon Config 开始跟踪其 Amazon 托管策略的更改。	2021 年 4 月 1 日

分配给的 IAM 角色的权限 Amazon Config

IAM 角色允许您定义一组权限。 Amazon Config 担任您分配给它的角色来写入您的 S3 存储桶、发布到您的 SNS 主题以及发出`Describe`或 `List` API 请求以获取 Amazon 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 Amazon Config 控制台创建或更新 IAM 角色时， Amazon Config 会自动为您附加所需的权限。有关更多信息，请参阅 使用控制台设置 Amazon Config。

> ⚠ 策略与合规结果
>
> IAM 策略和 Amazon Organizations中管理的其他策略可能会影响 Amazon Config 是否有权记录资源的配置更改。此外，规则会直接评估资源的配置，且执行评估时不会考虑这些策略。确保现行策略与您打算使用 Amazon Config的方式保持一致。

目录

- 创建 IAM 角色策略
  - 将 IAM 信任策略添加到您的角色
  - 用于 S3 存储桶的 IAM 角色策略
  - KMS 密钥的 IAM 角色策略
  - 用于 Amazon SNS 主题的 IAM 角色策略
  - 用于获取配置详细信息的 IAM 角色策略
  - 管理 S3 存储桶记录的权限

创建 IAM 角色策略

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

如果您使用 Amazon CLI 进行设置 Amazon Config 或更新现有 IAM 角色，则必须手动更新策略以允许 Amazon Config 访问您的 S3 存储桶、发布到您的 SNS 主题并获取有关您的资源的配置详细信息。

将 IAM 信任策略添加到您的角色

您可以创建一个 IAM 信任策略，该策略 Amazon Config 允许代入角色并使用它来跟踪您的资源。有关信任策略的更多信息，请参阅《IAM 用户指南》中的角色术语和概念。

以下是 Amazon Config 角色的信任策略示例：

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

您可以使用上述 IAM 角色信任关系中的 `AWS:SourceAccount` 条件来限制 Config 服务主体，仅在代表特定账户执行操作时与 Amazon IAM 角色进行交互。

Amazon Config 还支持这样的`AWS:SourceArn`条件，即限制 Config 服务委托人只能在代表拥有账户执行操作时担任 IAM 角色。使用 Amazon Config 服务主体时，该`AWS:SourceArn`属性将始终设置为`arn:aws:config:sourceRegion:sourceAccountID:*`客户管理的配置记录器的区域，以及`sourceAccountID`包含客户管理的配置记录器的帐户的 ID。`sourceRegion`

例如，添加以下条件限制 Config 服务主体只能代表账户 123456789012 中 us-east-1 区域中客户管理的配置记录器代入 IAM 角色："ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}。

用于 S3 存储桶的 IAM 角色策略

以下示例策略授予访问您的 S3 存储桶的 Amazon Config 权限：

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket"
    }
  ]
}
```

KMS 密钥的 IAM 角色策略

以下示例策略授予对新对象使用基于 KMS 的加密以进行 S3 存储桶交付的 Amazon Config 权限：

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
        }
    ]
}
```

用于 Amazon SNS 主题的 IAM 角色策略

以下示例策略授予访问您的 SNS 主题的 Amazon Config 权限：

JSON

```
{
  "Version":"2012-10-17",
  "Statement":
   [
     {
      "Effect":"Allow",
      "Action":"sns:Publish",
      "Resource":"arn:aws:sns:us-east-1:123456789012:MyTopic"
     }
    ]
}
```

如果您的 SNS 主题已加密，要了解更多设置说明，请参阅《Amazon Simple Notification Service 开发人员指南》中的配置 Amazon KMS 权限。

用于获取配置详细信息的 IAM 角色策略

建议使用 Amazon Config 服务相关角色:AWSServiceRoleForConfig。服务相关角色是预定义的，包括调用其他 Amazon Web Services 服务角色 Amazon Config 所需的所有权限。与 Amazon Config 服务相关的配置记录器需要服务相关角色。有关更多信息，请参阅为 Amazon Config使用服务相关角色。

如果您使用控制台创建或更新角色，请AWSServiceRoleForConfig为您 Amazon Config 附加。

如果您使用 Amazon CLI，请使用attach-role-policy命令并为以下项指定 Amazon 资源名称 (ARN)：AWSServiceRoleForConfig

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

管理 S3 存储桶记录的权限

Amazon Config 在创建、更新或删除 S3 存储桶时记录和发送通知。

建议使用 Amazon Config 服务相关角色:AWSServiceRoleForConfig。服务相关角色是预定义的，包括调用其他 Amazon Web Services 服务角色 Amazon Config 所需的所有权限。与 Amazon Config 服务相关的配置记录器需要服务相关角色。有关更多信息，请参阅为 Amazon Config使用服务相关角色。

更新客户管理的配置记录器的 IAM 角色

您可以更新客户管理的配置记录器使用的 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。您必须将策略附加到新角色，以 Amazon Config 授予记录配置并将其传送到您的交付渠道的权限。

有关创建 IAM 角色并将所需策略附加到 IAM 角色的信息，请参阅 步骤 3：创建 IAM 角色

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

更新 IAM 角色

您可以使用 Amazon Web Services 管理控制台 或更新您的 IAM 角色 Amazon CLI。

To update the IAM role (Console)

1. 登录 Amazon Web Services 管理控制台 并在家中打开https://console.aws.amazon.com/config/主 Amazon Config机。
2. 在导航窗格中，选择设置。
3. 在客户管理的记录器选项卡上，选择“设置”页面上的编辑。
4. 在数据治理部分中，为 Amazon Config以下角色选择 IAM 角色：
   - 使用现有的 Amazon Config 服务相关角色- Amazon Config 创建具有所需权限的角色。
   - 从您的账户选择一个角色：对于现有角色，选择您账户中的 IAM 角色。
5. 选择保存。

To update the IAM role (Amazon CLI)

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

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

Amazon Config 传送渠道的 Amazon S3 存储桶的权限

> **Important**
>
> 本页介绍的是为 Amazon Config 配送渠道设置 Amazon S3 存储桶。此页面与 Amazon Config 配置记录器可以记录的`AWS::S3::Bucket`资源类型无关。

默认情况下，Amazon S3 存储桶和对象都是私有的。 Amazon Web Services 账户 只有创建存储桶的人（资源所有者）才有访问权限。资源所有者可以通过创建访问策略来向其他资源和用户授予访问权限。

Amazon Config 自动为您创建 S3 存储桶时，它会添加所需的权限。但是，如果您指定现有 S3 存储桶，则必须手动添加这些权限。

主题

- 使用 IAM 角色时 Amazon S3 存储桶的必需权限
- 使用服务相关角色时 Amazon S3 Bucket 存储桶的必需权限
- 授予 Amazon Config 对 Amazon S3 存储桶的访问权限
- 跨账户传输时 Amazon S3 存储桶的必需权限

使用 IAM 角色时 Amazon S3 存储桶的必需权限

Amazon Config 使用您分配给配置记录器的 IAM 角色将配置历史记录和快照传送到您账户中的 S3 存储桶。对于跨账户交付， Amazon Config 首先尝试使用分配的 IAM 角色。如果存储桶策略未授予 `WRITE` 对 IAM 角色的访问权限，则 Amazon Config 将使用 `config.amazonaws.com` 服务主体。存储桶策略必须授予对 `config.amazonaws.com` 的 `WRITE` 访问权限才能完成传输。成功交付后，Amazon Config 保留其向跨账户 S3 存储桶交付的所有对象的所有权。

Amazon Config 使用您分配给配置记录器的 IAM 角色调用 Amazon S3 HeadBucketAPI，以确认 S3 存储桶是否存在及其位置。如果您没有必要的确认权限，则会在 Amazon CloudTrail 日志中看到`AccessDenied`错误。 Amazon Config 但是，即使没有必要的权限来确认 S3 存储桶 Amazon Config 是否存在及其位置，仍然 Amazon Config 可以提供配置历史记录和快照。

> **最小权限**
>
> Amazon S3 `HeadBucket` API 需要执行 `s3:ListBucket` 操作。

使用服务相关角色时 Amazon S3 Bucket 存储桶的必需权限

Amazon Config 服务相关角色无权将对象放入 Amazon S3 存储桶。如果您 Amazon Config 使用服务相关角色进行设置，则 Amazon Config 将使用`config.amazonaws.com`服务主体来提供配置历史记录和快照。您的账户或跨账户目标中的 S3 存储桶策略必须包括 Amazon Config 服务委托人写入对象的权限。

授予 Amazon Config 对 Amazon S3 存储桶的访问权限

完成以下步骤，启用 Amazon Config 将配置历史记录和快照传送到 Amazon S3 存储桶。

1. Amazon Web Services 管理控制台 使用拥有 S3 存储桶的账户登录。
2. 打开 Amazon S3 控制台，网址为 https://console.aws.amazon.com/s3/。
3. 选择 Amazon Config 要用于传送配置项目的存储桶，然后选择 Propert ie s。

4. 选择权限。
5. 选择 Edit Bucket Policy。
6. 将以下策略复制到 Bucket Policy Editor 窗口中：

> ⚠ 安全最佳实践
>
> 强烈建议您使用 AWS:SourceAccount 条件限制存储桶策略中的访问权限。这样可以确保 Amazon Config 仅代表预期用户授予访问权限。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
```

```
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

7. 替换存储桶策略中的以下值：

   - *amzn-s3-demo-bucket*— 用于传送配置历史记录和快照的 Amazon Config Amazon S3 存储桶的名称。
   - *[optional] prefix*— Amazon S3 对象密钥的可选补充，可帮助在存储桶中创建类似文件夹的组织。
   - *sourceAccountID*— Amazon Config 将在其中提供配置历史记录和快照的账户的 ID。

8. 选择 Save，然后选择 Close。

该AWS:SourceAccount条件将 Amazon Config 操作限制在指定 Amazon Web Services 账户范围内。对于组织内部向单个 S3 存储桶交付的多账户配置，请使用带有 Amazon Organizations 条件密钥的 IAM 角色而不是与服务相关的角色。例如 AWS:PrincipalOrgID。有关更多信息，请参阅《Amazon Organizations 用户指南》中的管理组织的访问权限。

该AWS:SourceArn条件将 Amazon Config 操作限制在指定的交付渠道内。AWS:SourceArn 格式如下所示：arn:aws:config:*sourceRegion*:*123456789012*。

例如，要将账户 123456789012 的 S3 存储桶访问权限限制为美国东部（弗吉尼亚州北部）区域的传输通道，可添加以下条件：

```
"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:"}
```

跨账户传输时 Amazon S3 存储桶的必需权限

当配置 Amazon Config 为将配置历史记录和快照传送到不同账户（跨账户设置）中的 Amazon S3 存储桶时，如果配置记录器和为交付通道指定的 S3 存储桶不同 Amazon Web Services 账户，则需要以下权限：

- 您分配给配置记录器的 IAM 角色需要明确的权限才能执行 `s3:ListBucket` 操作。这是因为使用此 IAM 角色 Amazon Config 调用 Amazon S3 HeadBucketAPI 来确定存储桶的位置。
- S3 存储桶策略必须包括分配给配置记录器的 IAM 角色的权限。

下面是一个示例存储桶策略配置：

```
{
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IAM Role-Arn assigned to the configuration recorder"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
}
```

Amazon Config 交付渠道 KMS 密钥的权限

如果您想为 S3 存储桶的 Amazon KMS 密钥创建策略，允许您对由 Amazon Config S3 存储桶交付的对象使用基于 KMS 的加密，请使用本主题中的信息。

目录

- 使用 IAM 角色（S3 存储桶传输）时 KMS 密钥的必需权限
- 使用服务相关角色时 Amazon KMS 密钥所需的权限（S3 存储桶交付）
- 授予对 Amazon KMS 密钥的 Amazon Config 访问权限

使用 IAM 角色（S3 存储桶传输）时 KMS 密钥的必需权限

如果您 Amazon Config 使用 IAM 角色进行设置，则可以将以下权限策略附加到 KMS 密钥：

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> 如果 IAM 角色、Amazon S3 存储桶策略或 Amazon KMS 密钥未提供对 Amazon Config的适当访问权限 Amazon Config，则尝试向 Amazon S3 存储桶发送配置信息将失败。在这种情况下，再次 Amazon Config 发送信息，这次是作为 Amazon Config 服务主体。在这种情况下，您必须将下文提到的权限策略附加到 Amazon KMS 密钥，以授予在向 Amazon S3 存储桶传送信息时使用该密钥的 Amazon Config 权限。

使用服务相关角色时 Amazon KMS 密钥所需的权限（S3 存储桶交付）

Amazon Config 服务相关角色无权访问 Amazon KMS 密钥。因此，如果您 Amazon Config 使用服务相关角色进行设置，则 Amazon Config 将改为以 Amazon Config 服务主体身份发送信息。您需要在 Amazon KMS 密钥上附加访问策略（如下所述），以授予在向 Amazon S3 存储桶传送信息时使用该 Amazon KMS 密钥的 Amazon Config 权限。

授予对 Amazon KMS 密钥的 Amazon Config 访问权限

此策略 Amazon Config 允许在向 Amazon S3 存储桶传送信息时使用 Amazon KMS 密钥

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

替换密钥策略中的以下值：

- *myKMSKeyARN*— 用于加密 Amazon Config 将向其传送配置项目的 Amazon S3 存储桶中数据的 Amazon KMS 密钥的 ARN。
- *sourceAccountID*— Amazon Config 将向其传送配置项目的账户的 ID。

您可以使用上述 Amazon KMS 密钥策略中的`AWS:SourceAccount`条件来限制 Config 服务主体仅在代表特定账户执行操作时与 Amazon KMS 密钥交互。

Amazon Config 还支持这样的`AWS:SourceArn`条件，即限制 Config 服务委托人仅在代表特定 Amazon Config 交付渠道执行操作时与 Amazon S3 存储桶进行交互。使用 Amazon Config 服务主体时，该`AWS:SourceArn`属性将始终设置为交付渠道`arn:aws:config:sourceRegion:sourceAccountID:*`所在`sourceRegion`区域，并且`sourceAccountID`是包含配送渠道的账户的 ID。有关 Amazon Config 配送渠道的更多信息，

请参阅管理交付渠道。例如，添加以下条件以限制 Config 服务主体仅代表账户 123456789012 中 us-east-1 区域中的传输通道与您的 Amazon S3 存储桶进行交互："ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}。

Amazon SNS 主题的权限

> **不支持加密的 Amazon SNS**
>
> Amazon Config 不支持加密的 Amazon SNS 主题。

本主题介绍如何配置 Amazon Config 以交付由其他账户拥有的 Amazon SNS 主题。 Amazon Config 必须具有向 Amazon SNS 主题发送通知所需的权限。

当 Amazon Config 控制台为您创建新的 Amazon SNS 主题时，会 Amazon Config 授予必要的权限。如果您选择现有 Amazon SNS 主题，请确保 Amazon SNS 主题包含所需的权限并遵循安全最佳实践。

> **不支持跨区域的 Amazon SNS 主题**
>
> Amazon Config 目前仅支持在同一个账户内 Amazon Web Services 区域 和跨账户进行访问。

目录

- 使用 IAM 角色时 Amazon SNS 主题的必需权限
- 使用服务相关角色时 Amazon SNS 主题的必需权限
- 授予 Amazon Config 对 Amazon SNS 主题的访问权限
- Amazon SNS 主题故障排除

使用 IAM 角色时 Amazon SNS 主题的必需权限

您可以将权限策略附加到不同账户拥有的 Amazon SNS 主题。如果要使用另一个账户中的 Amazon SNS 主题，请确保将以下策略附加到现有 Amazon SNS 主题。

```
{
  "Id": "Policy_ID",
```

```
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

对于Resource密钥，*account-id*是主题所有者的 Amazon 账号。对于*account-id1account-id2account-id3*、和，使用将数据发送 Amazon Web Services 账户 到 Amazon SNS 主题的。您可以用适当的值代替*region*和*myTopic*。

向 Amazon SNS 主题 Amazon Config 发送通知时，它会首先尝试使用 IAM 角色，但是如果该角色或 Amazon Web Services 账户 没有向该主题发布的权限，则尝试会失败。在这种情况下，将再次 Amazon Config 发送通知，这次是以 Amazon Config 服务主体名称 (SPN) 的形式发送。发布成功之前，主题的访问策略必须授予 `sns:Publish` 对 `config.amazonaws.com` 主体名称的访问权限。如果 IAM 角色无权向 Amazon SNS 主题发布内容，则必须按下一节中所述，在 Amazon SNS 主题中附加访问策略，以授予 Amazon Config 访问该主题的权限。

使用服务相关角色时 Amazon SNS 主题的必需权限

Amazon Config 服务相关角色无权访问 Amazon SNS 主题。因此，如果您 Amazon Config 使用服务相关角色 (SLR) 进行设置，则 Amazon Config 将改为以 Amazon Config 服务主体身份发送信息。您需要在 Amazon SNS 主题中附加访问策略（如下所述），才能授予向亚马逊 SNS 主题发送信息的 Amazon Config 权限。

对于同账户设置，当 Amazon SNS 主题和 SLR 位于同一账户中，并且 Amazon SNS 策略授予 SLR“`sns:Publish`”权限时，您无需使用 Amazon Config SPN。以下权限策略和安全最佳实践建议适用于跨账户设置。

授予 Amazon Config 对 Amazon SNS 主题的访问权限

此政策 Amazon Config 允许向 Amazon SNS 主题发送通知。要授予从其他账户 Amazon Config 访问 Amazon SNS 主题的权限，您需要附加以下权限策略。

> **Note**
>
> 作为安全最佳实践，强烈建议通过限制对`AWS:SourceAccount`条件中列出的帐户的访问来确保 Amazon Config 仅代表预期用户访问资源。

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

对于`Resource`密钥，*account-id*是主题所有者的 Amazon 账号。对于*account-id1*、*account-id2*、和*account-id3*，使用将数据发送 Amazon Web Services 账户 到 Amazon SNS 主题的。您可以用适当的值代替*region*和*myTopic*。

在代表特定账户执行操作时，您可以使用之前的 Amazon SNS 主题政策中的`AWS:SourceAccount`条件来限制 Amazon Config 服务主体名称 (SPN) 只能与 Amazon SNS 主题进行交互。

Amazon Config 还支持将 Amazon Config 服务主体名称 (SPN) 限制为仅在代表特定 Amazon Config 交付渠道执行操作时与 S3 存储桶交互的`AWS:SourceArn`条件。使用 Amazon Config 服务主体名称 (SPN) 时，该`AWS:SourceArn`属性将始终设置为交付渠道的区域`arn:aws:config:sourceRegion:sourceAccountID:*`在哪里`sourceRegion`，并且`sourceAccountID`是包含配送渠道的账户的 ID。有关 Amazon Config 交付渠道的更多信息，请参阅管理交付渠道。例如，添加以下条件以限制 Amazon Config 服务主体名称 (SPN) 仅代表账户中`us-east-1`该地区的交付渠道与您的 S3 存储桶进行交互`123456789012`：`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`。

Amazon SNS 主题故障排除

Amazon Config 必须拥有向 Amazon SNS 主题发送通知的权限。如果 Amazon SNS 主题无法收到通知，请验证所担任 Amazon Config 的 IAM 角色是否具有所需的`sns:Publish`权限。

对 Amazon Config 身份和访问进行故障排除

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

主题

- 我无权在以下位置执行操作 Amazon Config
- 我无权执行 iam：PassRole
- 我想允许我以外的人 Amazon Web Services 账户 访问我的 Amazon Config 资源

我无权在以下位置执行操作 Amazon Config

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

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

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

在此情况下，Mateo 的策略必须更新以允许其使用 `config:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 iam:PassRole 操作，则必须更新策略以允许您将角色传递给。 Amazon Config

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

当名为 marymajor 的 IAM 用户尝试使用控制台在 Amazon Config中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

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

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 Amazon Web Services 账户 访问我的 Amazon Config 资源

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

要了解更多信息，请参阅以下内容：

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

将服务相关角色用于 Amazon Config

Amazon Config 使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 Amazon Config服务相关角色由服务预定义 Amazon Config ，包括该服务代表您调用其他 Amazon 服务所需的所有权限。

服务相关角色使设置变得 Amazon Config 更加容易，因为您不必手动添加必要的权限。 Amazon Config 定义其服务相关角色的权限，除非另有定义，否则 Amazon Config 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其他 IAM 实体。

有关支持服务相关角色的其他服务的信息，请参阅使用 IAM 的Amazon 服务并查找 Service-Linked Role（服务相关角色）列中显示为 Yes（是）的服务。选择是和链接，查看该服务的服务关联角色文档。

的服务相关角色权限 Amazon Config

Amazon Config 使用名为的服务相关角色 AwsServiceRoleForConfig— Amazon Config 使用此服务相关角色代表您调用其他 Amazon 服务。要查看最新更新，请参阅 the section called “策略更新”

AwsServiceRoleForConfig 服务关联角色信任 `config.amazonaws.com` 服务来代入角色。

该`AwsServiceRoleForConfig`角色的权限策略包含 Amazon Config 资源的只读和只写权限，以及其他支持的服务中资源的只读权限。 Amazon Config 要查看的托管策略 AwsServiceRoleForConfig，请参阅的Amazon 托管策略 Amazon Config。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。有关更多信息，请参阅《IAM 用户指南》中的服务关联角色权限。

要将服务相关角色与配合使用 Amazon Config，您必须在 Amazon S3 存储桶和 Amazon SNS 主题上配置权限。有关更多信息，请参阅 使用服务相关角色时 Amazon S3 Bucket 存储桶的必需权限、使用服务相关角色时 Amazon KMS 密钥所需的权限（S3 存储桶交付） 和 使用服务相关角色时 Amazon SNS 主题的必需权限。

为创建服务相关角色 Amazon Config

在 IAM CLI 或 IAM API 中，用 `config.amazonaws.com` 服务名称创建一个服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。如果您删除了此服务相关角色，可以使用同样的过程再次创建角色。

编辑的服务相关角色 Amazon Config

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

删除的服务相关角色 Amazon Config

如果不再需要使用某个需要服务关联角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

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

要删除使用的 Amazon Config 资源 AwsServiceRoleForConfig

确保您没有使用服务相关角色的。ConfigurationRecorders您可以使用 Amazon Config 控制台停止配置记录器。要停止记录，请选择 Recording is on（记录已打开）下的 Turn off（关闭）。

您可以删除ConfigurationRecorder正在使用的 Amazon Config API。要删除，请使用 delete-configuration-recorder 命令。

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

使用 IAM 手动删除服务关联角色

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

中的事件响应 Amazon Config

Amazon非常重视安全性。作为 Amazon 云责任共担模式的一部分， Amazon 管理满足大多数安全敏感组织要求的数据中心、网络和软件架构。 Amazon 负责与 Amazon Config 服务本身有关的任何事

件响应。此外，作为 Amazon 客户，您也有责任维护云端的安全。这意味着您可以从自己有权访问的 Amazon 工具和功能中控制您选择实施的安全性，并负责在责任共担模型中对事件做出响应。

通过建立符合云端运行应用程序目标的安全基准，您可以检测出可以响应的偏差。由于安全事件响应可能是一个复杂的主题，因此我们鼓励您查看以下资源，以便更好地了解事件响应 (IR) 和您的选择对企业目标的影响：Amazon 安全事件响应指南、Amazon 安全最佳实践白皮书和Amazon 云采用框架 (CAF) 的安全视角白皮书。

的合规性验证 Amazon Config

Amazon Config 作为多个合规计划的一部分，第三方审计师对安全性和 Amazon 合规性进行评估。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

要了解是否属于特定合规计划的范围，请参阅Amazon Web Services 服务 “” Amazon Web Services 服务 中的 “按合规计划划分的范围”，然后选择您感兴趣的合规计划。 Amazon Web Services 服务 有关一般信息，请参阅合规计划。

您可以使用下载第三方审计报告 Amazon Artifact。有关更多信息，请参阅中的 “下载报告” Amazon Artifact。

您在使用 Amazon Web Services 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。有关您在使用时的合规责任的更多信息 Amazon Web Services 服务，请参阅Amazon 安全文档。

韧性在 Amazon Config

Amazon 全球基础设施是围绕 Amazon 区域和可用区构建的。 Amazon 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 Amazon 区域和可用区的更多信息，请参阅Amazon 全球基础设施。

中的基础设施安全 Amazon Config

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

您可以使用 Amazon 已发布的 API 调用 Amazon Config 通过网络进行访问。客户端必须支持以下内容：

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

配置和漏洞分析

对于 Amazon Config， Amazon 处理基本的安全任务，例如客户机操作系统 (OS) 和数据库修补、防火墙配置和灾难恢复。

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有某操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 Amazon，跨服务模仿可能会导致混乱的副手问题。一个服务（呼叫服务）调用另一项服务（所谓的服务）时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为防止这种情况， Amazon 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用aws:SourceArn和aws:SourceAccount全局条件上下文密钥来限制为资源 Amazon Config 提供其他服务的权限。如果您只希望将一个资源与跨服务访问相关联，请使用。aws:SourceArn如果您想允许该账户中的任何资源与跨服务使用操作相关联，请使用。aws:SourceAccount

防范混淆代理问题最有效的方法是使用 aws:SourceArn 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 ARN，或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符字符（*）的 aws:SourceArn 全局上下文条件键。例如 arn:aws:*servicename*:*:*123456789012*:*。

如果 aws:SourceArn 值不包含账户 ID，例如 Amazon S3 存储桶 ARN，您必须使用两个全局条件上下文键来限制权限。

以下示例显示了如何使用中的aws:SourceArn和aws:SourceAccount全局条件上下文密钥 Amazon Config 来防止出现混淆的副手问题：授予 Amazon Config 对 Amazon S3 存储桶的访问权限。

的安全最佳实践 Amazon Config

Amazon Config 提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

- 利用标记 Amazon Config，这样可以更轻松地管理、搜索和筛选资源。
- 确认您的配送渠道已正确设置，确认后，请验证是否正确录制。 Amazon Config

有关更多信息，请参阅 Amazon Config 最佳实践博客。

登录和监控Amazon Config

Amazon Config与Amazon CloudTrail一项服务集成，该服务提供用户、角色或Amazon服务在中执行的操作的记录Amazon Config。监控是维护Amazon解决方案的可靠性、可用性和性能的重要组成部分。Amazon Config

主题

- 使用记录Amazon Config API 调用Amazon CloudTrail
- 监控

使用记录Amazon Config API 调用Amazon CloudTrail

CloudTrail 将所有 API 调用捕获Amazon Config为事件。捕获的调用包括来自Amazon Config控制台的调用和对Amazon Config API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件Amazon Config。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向哪个请求发出Amazon Config、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅《Amazon CloudTrail用户指南》。

主题

- Amazon Config中的信息 CloudTrail
- 了解Amazon Config日志文件条目
- 示例日志文件

Amazon Config中的信息 CloudTrail

CloudTrail 在您创建账户Amazon Web Services 账户时已在您的账户上启用。当活动发生在中时Amazon Config，该活动会与其他Amazon服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件Amazon Web Services 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的Amazon Web Services 账户事件（包括的事件）Amazon Config，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有Amazon Web Services 区域。跟踪记录Amazon分区中所有区域的事件，并将

日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他Amazon服务，以进一步分析 CloudTrail 日志中收集的事件数据并对其采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 为其配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

所有Amazon Config操作均由《API 参考》记录 CloudTrail 并记录在《Amazon Config API 参考》中。例如，对DeliverConfigSnapshotDeleteDeliveryChannel、和DescribeDeliveryChannels操作的调用会在 CloudTrail 日志文件中生成条目。

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

- 请求是使用根证书还是Amazon Identity and Access Management(IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他Amazon服务发出。

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

了解Amazon Config日志文件条目

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

示例日志文件

有关 CloudTrail 日志条目的示例，请参阅以下主题。

DeleteDeliveryChannel

以下是该DeleteDeliveryChannel操作的 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

以下是该DeliverConfigSnapshot操作的 CloudTrail 日志文件示例。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
```

```
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

以下是该DescribeConfigurationRecorderStatus操作的 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

以下是该DescribeConfigurationRecorders操作的 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

以下是该DescribeDeliveryChannels操作的 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

以下是该GetResourceConfigHistory操作的 CloudTrail 日志文件示例。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
```

```
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "GetResourceConfigHistory",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "resourceId": "vpc-a12bc345",
        "resourceType": "AWS::EC2::VPC",
        "limit": 0,
        "laterTime": "Dec 11, 2014 12:58:42 AM",
        "earlierTime": "Dec 10, 2014 4:58:42 PM"
      },
      "responseElements": null,
      "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111111111111"
      }
```

PutConfigurationRecorder

以下是该PutConfigurationRecorder操作的 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

以下是该PutDeliveryChannel操作的 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": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

以下是该StartConfigurationRecorder操作的 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": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```


StopConfigurationRecorder

以下是该StopConfigurationRecorder操作的 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"
  }
```


监控

您可以使用其他Amazon服务来监控Amazon Config资源。

- 每次由于用户 API 活动而创建、更新或以其他方式修改支持的Amazon资源时，您都可以使用亚马逊简单通知服务 (SNS) Simple Notification Service 向您发送通知。
- 您可以使用 Amazon EventBridge 来检测Amazon Config事件状态的变化并做出反应。

主题

- 使用 Amazon SQS 监控Amazon资源变化
- 使用 Amazon EventBridge 监控 Amazon Config

使用 Amazon SQS 监控Amazon资源变化

Amazon Config每次由于用户 API 活动而创建、更新或以其他方式修改支持的Amazon资源时，都会使用亚马逊简单通知服务 (SNS) Simple Notification Service 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，您可能认为知道何时有人修改安全组的配置至关重要，但不必每次更改您的 Amazon EC2 实例上的标签时都要知道。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。如果您想通过这些或其他方式以编程方式使用来自Amazon Config的数据，请使用亚马逊简单队列服务队列作为 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 端点的通知消息。

无论每个区域只订阅一个主题还是每个区域的每个账户只订阅一个主题，您都可以使用单个 SQS 队列订阅多个主题。您必须用队列订阅您需要的 SNS 主题。(您可以用多个队列订阅一个 SNS 主题。）有关更多信息，请参阅将 Amazon SNS 消息发送到 Amazon SQS 队列。

Amazon SQS 的权限

要将 Amazon SQS 与配合使用Amazon Config，您必须配置一项策略，向您的账户授予执行所有 SQS 队列允许的操作的权限。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。

JSON

```
{
  "Version":"2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
        },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

您还必须创建一项策略，授予 SNS 主题和订阅该主题的 SQS 队列之间的连接权限。以下是一个策略示例，它允许使用亚马逊资源名称 (ARN) 的 SNS 主题 arn: aws: sns: us-east-2:111122223333: test-topic 对名为 arn: aws: sqs: us-east-2:111122223333: 的队列执行任何操作。test-topic-queue

> **Note**
>
> SNS 主题和 SQS 队列的账户必须处于同一区域中。

JSON

```
{
  "Version":"2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

每项策略中的规定可以只针对一个队列而不是多个队列。有关 Amazon SQS 策略受到的其他限制的信息，请参阅 Amazon SQS 策略的特别信息。

使用 Amazon EventBridge 监控 Amazon Config

Amazon EventBridge 提供近乎实时的系统事件流，这些系统事件描述了 Amazon 资源中的更改。可以使用 Amazon EventBridge 检测 Amazon 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 EventBridge 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 Amazon Config 创建事件规则之前，您应当执行以下操作：

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

主题

- 注意事项
- Amazon Config 的 Amazon EventBridge 格式
- 为 Amazon Config 创建 Amazon EventBridge 规则

注意事项

如果您不使用 Amazon Config 记录以下资源类型，则不会通过 EventBridge 收到这些资源类型的警报：

- `AWS::ACM::Certificate`
- `AWS::CloudTrail::Trail`
- `AWS::CloudWatch::Alarm`
- `AWS::EC2::CustomerGateway`
- `AWS::EC2::EIP`
- `AWS::EC2::Host`
- `AWS::EC2::Instance`
- `AWS::EC2::InternetGateway`
- `AWS::EC2::NetworkAcl`
- `AWS::EC2::NetworkInterface`
- `AWS::EC2::RouteTable`
- `AWS::EC2::SecurityGroup`
- `AWS::EC2::Subnet`
- `AWS::EC2::VPC`
- `AWS::EC2::VPNConnection`
- `AWS::EC2::VPNGateway`

- AWS::EC2::Volume
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::IAM::Group
- AWS::IAM::Policy
- AWS::IAM::Role
- AWS::IAM::User
- AWS::RDS::DBInstance
- AWS::RDS::DBSecurityGroup
- AWS::RDS::DBSnapshot
- AWS::RDS::DBSubnetGroup
- AWS::RDS::EventSubscription
- AWS::Redshift::Cluster
- AWS::Redshift::ClusterParameterGroup
- AWS::Redshift::ClusterSecurityGroup
- AWS::Redshift::ClusterSnapshot
- AWS::Redshift::ClusterSubnetGroup
- AWS::Redshift::EventSubscription
- AWS::S3::Bucket

Amazon Config 的 Amazon EventBridge 格式

Amazon Config 的 EventBridge 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 Amazon Config 创建 Amazon EventBridge 规则

可使用以下步骤创建对 Amazon Config 发出的事件进行触发的 EventBridge 规则。尽最大努力发出事件。

1. 在导航窗格中，选择规则。
2. 选择创建规则。
3. 为规则输入名称和描述。

   规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。

   > **Note**
   >
   > 事件总线从源接收事件，通过规则对事件进行评估，应用所有已配置的输入转换，然后将事件路由至相应的一个或多个目标。您的账户有一个默认事件总线，它接收来自 Amazon Web Services 服务的事件。自定义事件总线可以从您的自定义应用程序和服务接收事件。合作伙伴事件总线从 SaaS 合作伙伴创建的事件源接收事件。这些事件来自合作伙伴的服务或应用程序。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 中的事件总线。

4. 对于规则类型，选择具有事件模式的规则。
5. 对于事件源，选择 Amazon 事件或 EventBridge 合作伙伴事件。
6. （可选）对于示例事件类型，选择 Amazon 事件。
7. （可选）对于示例事件，选择用于触发此规则的事件类型：
   - 选择通过 CloudTrail 进行的 Amazon API 调用，以使规则基于对此服务进行的 API 调用。有关创建此类规则的更多信息，请参阅教程：为 Amazon CloudTrail API 调用创建 Amazon EventBridge 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。

     如以下支持文章中所述，在创建或删除资源时，可以使用 EventBridge 来接收自定义电子邮件通知：当使用 Amazon Config 服务在我的 Amazon Web Services 账户中创建资源时，我如何接收

自定义电子邮件通知？和当使用 Amazon Config 服务删除我的 Amazon Web Services 账户中的资源时，我如何接收自定义电子邮件通知？。

- 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。

  如以下支持文章中所述，当资源不合规时，可以使用 EventBridge 来接收自定义电子邮件通知：当使用 Amazon Config 的 Amazon 资源不合规时，如何通知我？。
- 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。

8. 对于创建方法，选择使用模式表单。
9. 对于事件源，选择Amazon 服务。
10. 对于 Amazon 服务，请选择 Config。
11. 对于事件类型，选择用于触发此规则的事件类型：
    - 选择所有事件以创建一个应用于所有 Amazon 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。
    - 选择通过 CloudTrail 进行的 Amazon API 调用，以使规则基于对此服务进行的 API 调用。有关创建此类规则的更多信息，请参阅教程：为 Amazon CloudTrail API 调用创建 Amazon EventBridge 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。

      如以下支持文章中所述，在创建或删除资源时，可以使用 EventBridge 来接收自定义电子邮件通知：当使用 Amazon Config 服务在我的 Amazon Web Services 账户中创建资源时，我如何接收自定义电子邮件通知？和当使用 Amazon Config 服务删除我的 Amazon Web Services 账户中的资源时，我如何接收自定义电子邮件通知？。
    - 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。

      如以下支持文章中所述，当资源不合规时，可以使用 EventBridge 来接收自定义电子邮件通知：当使用 Amazon Config 的 Amazon 资源不合规时，如何通知我？。
    - 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。
12. 选择 Any message type 以接收任何类型的通知。选择 Specific message type(s ） 以接收以下类型的通知：

- 如果选择 ConfigurationItemChangeNotification，当 Amazon Config 评估的资源的配置发生变化时，您将收到消息。
- 如果您选择 ComplianceChangeNotification，则会在 Amazon 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 Amazon 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 Amazon Config 成功将配置快照传送到 Amazon S3 存储桶时收到消息。
- 如果您选择 ConfigurationSnapshotDeliveryFailed，则会在 Amazon Config 无法将配置快照传送到 Amazon S3 存储桶时收到消息。
- 如果您选择 ConfigurationSnapshotDeliveryStarted，则会在 Amazon Config 开始将配置快照传送到 Amazon S3 存储桶时收到消息。
- 如果您选择 ConfigurationHistoryDeliveryCompleted，则会在 Amazon Config 成功将配置历史记录传送到 Amazon S3 存储桶时收到消息。

13如果您从事件类型下拉列表中选择了某个特定事件类型，请选择任何资源类型，以创建一个应用于 Amazon Config 支持的所有资源类型的规则。

或者，选择 Specific resource type(s)（特定资源类型），然后键入 Amazon Config 支持的资源类型（例如，`AWS::EC2::Instance`）。

14如果您从事件类型下拉列表中选择了某个特定事件类型，请选择任何资源 ID，以包括 Amazon Config 支持的任何资源 ID。

或者，选择 Specific resource ID(s)（特定资源 ID），然后键入 Amazon Config 支持的资源 ID（例如，`i-04606de676e635647`）。

15如果您从事件类型下拉列表中选择了某个特定事件类型，请选择任何规则名称，以包括 Amazon Config 支持的任何规则。

或者，选择 Specific rule name(s)（特定规则名称），然后键入 Amazon Config 支持的规则（例如，required-tags）。

16对于选择目标，选择您准备为此规则使用的目标类型，然后配置该类型所需的任何其他选项。

17显示的字段因您选择的服务而异。根据需要输入此目标类型的特定信息。

18对于许多目标类型，EventBridge 需要权限以便将事件发送到目标。在这些情况下，EventBridge 可以创建运行事件所需的 IAM 角色：

- 若要自动创建 IAM 角色，请选择 Create a new role for this specific resource（为此特定资源创建新角色）。

- 要使用您之前创建的 IAM 角色，请选择 Use existing role（使用现有角色）。

19.（可选）选择 Add target（添加目标），以便为此规则添加另一个目标。

20.（可选）为规则输入一个或多个标签。有关更多信息，请参阅 Amazon EventBridge 标签。

21.审查您的规则设置以确保其符合事件监控要求。

22选择创建以确认您的选择。

将 Amazon Config 与接口 Amazon VPC 端点一起使用

如果您使用 Amazon Virtual Private Cloud（Amazon VPC）托管 Amazon 资源，则可以在您的 VPC 和 Amazon Config 之间建立私有连接。您可以使用此连接从您的 VPC 上与 Amazon Config 通信而不用访问公共 Internet。

Amazon VPC 是一项 Amazon 服务，可用来启动在虚拟网络中定义的 Amazon 资源。借助 VPC，您可以控制您的网络设置，如 IP 地址范围、子网、路由表和网络网关。接口 VPC 端点由 Amazon PrivateLink 提供支持，后者是一种 Amazon 技术，可将弹性网络接口与私有 IP 地址结合使用来支持 Amazon 服务之间的私有通信。要将 VPC 连接到，Amazon Config请为 Amazon Config 定义一个接口 VPC 端点。这种类型的端点使您能够将 VPC 连接到Amazon服务。该端点提供了到 Amazon Config 的可靠、可扩展的连接，无需互联网网关、网络地址转换（NAT）实例或 VPN 连接。有关更多信息，请参阅 Amazon VPC 用户指南中的什么是 Amazon VPC。

以下步骤适用于 Amazon VPC 的用户。有关更多信息，请参阅 Amazon VPC 用户指南中的入门。

为 创建 VPC 端点Amazon Config

要开始将您的 Amazon Config 与 VPC 一起使用，请为 Amazon Config 创建接口 VPC 端点。您无需更改 Amazon Config 的设置。Amazon Config 将调用使用自身的公有终端节点的其他 Amazon 服务。有关更多信息，请参阅 Amazon VPC 用户指南中的创建接口终端节点。

常见问题

看不到我最新的配置更改

我可以立即查看我的配置更改吗？

Amazon Config 通常会在检测到更改后立即或按照您指定的频率记录您的资源配置更改。但是，这需要尽最大努力，有时可能需要更长的时间。如果问题在一段时间后仍然存在，请联系 Amazon Web Services 支持 并提供 Amazon CloudWatch 支持的 Amazon Config 指标。有关这些指标的信息，请参阅Amazon Config 使用情况和成功指标。

Amazon Config 中的间接关系

主题

- 什么是资源关系？
- 什么是与资源的直接关系和间接关系？
- Amazon Config 支持哪些间接关系？
- 哪些场景使用间接关系？
- 由于直接关系和间接关系，配置项是如何创建的？
- 由于间接关系而生成的配置项有哪些？
- 如何禁用间接关系？
- 如何检索与间接关系相关的配置数据？

什么是资源关系？

在 Amazon 中，资源是指可管理的实体，例如 Amazon Elastic Compute Cloud（Amazon EC2）实例、Amazon CloudFormation 堆栈或 Amazon S3 存储桶。Amazon Config 是一项服务，它会在每次检测到记录的资源类型更改时，通过创建配置项（CI）跟踪和监控资源，或者会以您设置的记录频率进行跟踪和监控。例如，将 Amazon Config 设置为跟踪 Amazon EC2 实例时，它会在每次创建、更新或删除实例时创建配置项。Amazon Config 创建的每个配置项都有多个字段，包括、`accountIdarn`（Amazon 资源名称）、`awsRegion`、`configuration`、`tags` 和 `relationships`。CI 的关系字段可让 Amazon Config 显示资源之间是如何相互关联的。例如，关系可能表示 ID 为 `vol-123ab45d` 的 Amazon EBS 卷已附加到 ID 为 `i-a1b2c3d4` 且与安全组 `sg-ef678hk` 关联的 Amazon EC2 实例。

什么是与资源的直接关系和间接关系？

Amazon Config 从配置字段中推导出大多数资源类型的关系，这些关系称为“直接”关系。直接关系是一个资源（A）和另一个资源（B）之间的单向连接（A→B），通常从资源（A）的描述 API 响应中获得。过去，对于 Amazon Config 最初支持的某些资源类型，它还会从其他资源的配置中捕获关系，从而创建双向（B→A）的“间接”关系。例如，Amazon EC2 实例与其安全组之间的关系是直接关系，因为安全组包含在 Amazon EC2 实例的描述 API 响应中。另一方面，安全组和 Amazon EC2 实例之间的关系是间接关系，因为描述安全组不会返回与其关联的实例的任何信息。

例如，间接关系有助于回答以下问题：

- 当 NAT 网关出现故障时，私有子网中的哪些 EC2 实例会受到影响？
- 如果修改了路由表，哪个 EC2 实例可能会遇到连接问题？
- 哪个安全组从未使用过？
- 附加到 EC2 实例的哪个辅助 ENI 与安全组相关联？

因此，当检测到资源配置更改时，Amazon Config 不仅会为该资源创建 CI，还会为任何相关资源（包括具有间接关系的资源）生成 CI。例如，当 Amazon Config 检测到 Amazon EC2 实例中的更改时，它会为该实例创建一个 CI，并为与该实例关联的安全组创建一个 CI。

Amazon Config 支持哪些间接关系？

Amazon Config 中支持以下间接资源关系。

资源类型	与此资源类型间接相关		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` ，`AWS::EC2::NetworkInterface` ，`AWS::EC2::Subnet` ，`AWS::EC2::VPNGateway` ，`AWS::EC2::VPC`		

资源类型	与此资源类型间接相关		
AWS::EC2::EIP	AWS::EC2::Instance ，AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup ，AWS::EC2::Subnet ，AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup ，AWS::EC2::Subnet ，AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet ，AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway ，AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		

资源类型	与此资源类型间接相关		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

哪些场景使用间接关系？

以下是使用间接关系的 Amazon 服务和相应服务的功能。

Amazon 功能	场景
Amazon Config 托管规则	ec2-security-group-attached-to-eni 规则检查弹性网络接口（ENI）是否关联了非默认安全组。 如果没有间接关系，则需要创建自定义规则来检查非默认安全组是否已附加到 ENI。
Amazon Firewall Manager	使用情况审计安全组策略使用间接关系来了解上次使用安全组的时间。 如果没有间接关系，则需要同时建立安全组并将其关联到新资源，以避免对 Amazon Firewall Manager 触发规则。

默认资源	• 创建非默认 VPC 时的默认资源：
	  • 默认安全组、默认网络 ACL 和默认路由表。
	• 创建默认 VPC 时的默认资源：
	  • 创建的所有资源均具有非默认 VPC、一个互联网网关，以及您有权访问的每个可用区中的默认子网。
	• 当账户首次调用 EC2 时，会自行创建默认 VPC。

Amazon 功能	场景
	• 将为新启动的可用区中的账户创建默认子网。 如果没有间接关系，您最多需要等待 12 小时，自动基准化功能才能记录默认资源的变更。

由于直接关系和间接关系，配置项是如何创建的？

对于资源之间的直接关系（A→B），对资源 B 的任何配置更改也将启动资源 A 的配置项（CI）。同样，对于间接关系（B→A），当资源 A 发生配置更改时，将为资源 B 生成一个新的 CI。例如，Amazon EC2 实例与安全组是直接关系，因此对安全组的任何配置更改都将为安全组生成一个 CI，并为 EC2 实例生成一个 CI。同样，安全组与 Amazon EC2 实例是间接关系，因此对 EC2 实例的任何配置更改都将为 Amazon EC2 实例生成一个 CI，并为安全组生成一个 CI。

由于间接关系而生成的配置项有哪些？

以下是由于间接资源关系而生成的其他配置项（CI）。

以下资源类型的配置更改	将为以下资源类型生成 CI		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` 、`AWS::EC2::NetworkInterface` `AWS::EC2::Subnet` 、`AWS::EC2::VPNGateway` 、和 `AWS::EC2::VPC`		
`AWS::EC2::EIP`	`AWS::EC2::Instance` ，`AWS::EC2:`		

以下资源类型的配置更改	将为以下资源类型生成 CI		
	:NetworkInterface		
AWS::EC2::Instance	AWS::EC2::SecurityGroup，AWS::EC2::Subnet，AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup，AWS::EC2::Subnet，AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet，AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway，AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		

以下资源类型的配置更改	将为以下资源类型生成 CI		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

如何禁用间接关系？

完成以下步骤以删除关系：

1. 使用您的账户或使用管理账户为多个账户开立 Amazon Web Services 支持 案例。
2. 选择技术作为支持类型。
3. 对于“服务”，选择 Amazon Config
4. 在“类别”中，选择其他。
5. 选择适当的严重级别。
6. 在主题行中输入禁用间接关系。
7. 在描述中：
   - 确认您已阅读此常见问题解答并想要继续。
   - 列出您要禁用间接关系的区域。
   - 如果通过管理账户提交，请包括账户 ID 及其关联区域。
   - 对于多个账户，您可以附加包含账户 ID 和区域的 CSV 文件。

Amazon Web Services 支持 工程师将提供后续步骤和状态更新。建议您维护一份禁用间接关系的 Amazon 账户和区域的列表。对于新账户，请提交新 Amazon Web Services 支持 案例以禁用间接关系。

如何检索与间接关系相关的配置数据？

您可以在 Amazon Config 高级查询中运行结构化查询语言（SQL）查询，以检索与间接资源关系相关的配置数据。例如，如果您想检索与安全组相关的 Amazon EC2 实例列表，请使用以下查询：

```
SELECT
    resourceId,
    resourceType
    WHERE
```

```
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

使用的代码示 Amazon Config 例 Amazon SDKs

以下代码示例说明如何 Amazon Config 使用 Amazon 软件开发套件 (SDK)。

操作是大型程序的代码摘录，必须在上下文中运行。您可以通过操作了解如何调用单个服务函数，还可以通过函数相关场景的上下文查看操作。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

代码示例

- 使用的基本示 Amazon Config 例 Amazon SDKs
  - 用于 Amazon Config 使用的操作 Amazon SDKs
    - DeleteConfigRule与 Amazon SDK 或 CLI 配合使用
    - 将 DescribeComplianceByConfigRule 与 CLI 配合使用
    - 将 DescribeComplianceByResource 与 CLI 配合使用
    - 将 DescribeConfigRuleEvaluationStatus 与 CLI 配合使用
    - DescribeConfigRules与 Amazon SDK 或 CLI 配合使用
    - 将 DescribeConfigurationRecorderStatus 与 CLI 配合使用
    - 将 DescribeConfigurationRecorders 与 CLI 配合使用
    - 将 DescribeDeliveryChannels 与 CLI 配合使用
    - 将 GetComplianceDetailsByConfigRule 与 CLI 配合使用
    - 将 GetComplianceDetailsByResource 与 CLI 配合使用
    - 将 GetComplianceSummaryByConfigRule 与 CLI 配合使用
    - 将 GetComplianceSummaryByResourceType 与 CLI 配合使用
    - PutConfigRule与 Amazon SDK 或 CLI 配合使用
    - 将 PutDeliveryChannel 与 CLI 配合使用

使用的基本示 Amazon Config 例 Amazon SDKs

以下代码示例说明如何使用 with 的基础 Amazon Config 知识 Amazon SDKs。

示例

- 用于 Amazon Config 使用的操作 Amazon SDKs

- DeleteConfigRule与 Amazon SDK 或 CLI 配合使用
- 将 DescribeComplianceByConfigRule 与 CLI 配合使用
- 将 DescribeComplianceByResource 与 CLI 配合使用
- 将 DescribeConfigRuleEvaluationStatus 与 CLI 配合使用
- DescribeConfigRules与 Amazon SDK 或 CLI 配合使用
- 将 DescribeConfigurationRecorderStatus 与 CLI 配合使用
- 将 DescribeConfigurationRecorders 与 CLI 配合使用
- 将 DescribeDeliveryChannels 与 CLI 配合使用
- 将 GetComplianceDetailsByConfigRule 与 CLI 配合使用
- 将 GetComplianceDetailsByResource 与 CLI 配合使用
- 将 GetComplianceSummaryByConfigRule 与 CLI 配合使用
- 将 GetComplianceSummaryByResourceType 与 CLI 配合使用
- PutConfigRule与 Amazon SDK 或 CLI 配合使用
- 将 PutDeliveryChannel 与 CLI 配合使用

用于 Amazon Config 使用的操作 Amazon SDKs

以下代码示例演示了如何使用执行单个 Amazon Config 操作 Amazon SDKs。每个示例都包含一个指向的链接 GitHub，您可以在其中找到有关设置和运行代码的说明。

以下示例仅包括最常用的操作。有关完整列表，请参阅 Amazon Config API 参考。

示例

- DeleteConfigRule与 Amazon SDK 或 CLI 配合使用
- 将 DescribeComplianceByConfigRule 与 CLI 配合使用
- 将 DescribeComplianceByResource 与 CLI 配合使用
- 将 DescribeConfigRuleEvaluationStatus 与 CLI 配合使用
- DescribeConfigRules与 Amazon SDK 或 CLI 配合使用
- 将 DescribeConfigurationRecorderStatus 与 CLI 配合使用
- 将 DescribeConfigurationRecorders 与 CLI 配合使用
- 将 DescribeDeliveryChannels 与 CLI 配合使用
- 将 GetComplianceDetailsByConfigRule 与 CLI 配合使用

- 将 GetComplianceDetailsByResource 与 CLI 配合使用
- 将 GetComplianceSummaryByConfigRule 与 CLI 配合使用
- 将 GetComplianceSummaryByResourceType 与 CLI 配合使用
- PutConfigRule与 Amazon SDK 或 CLI 配合使用
- 将 PutDeliveryChannel 与 CLI 配合使用

`DeleteConfigRule`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DeleteConfigRule`。

CLI

Amazon CLI

删除 C Amazon onfig 规则

以下命令删除名为的 Amazon Config 规则`MyConfigRule`：

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DeleteConfigRule中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
```

```
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅适用DeleteConfigRule于 Python 的Amazon SDK (Boto3) API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    lo_cfs->deleteconfigrule( iv_rule_name ).
    MESSAGE 'Deleted AWS Config rule.' TYPE 'I'.
```

- 有关 API 的详细信息，请参阅适用DeleteConfigRule于 S AP 的Amazon SDK ABAP API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeComplianceByConfigRule** 与 CLI 配合使用

以下代码示例演示如何使用 DescribeComplianceByConfigRule。

CLI

Amazon CLI

获取您的 Amazon Config 规则的合规性信息

以下命令返回一个或多个 Amazon 资源违反的每个 Amazon Config 规则的合规性信息：

```
aws configservice describe-compliance-by-config-rule --compliance-
types NON_COMPLIANT
```

在输出中，每个 CappedCount 属性的值都表示有多少资源不符合相关规则。例如，以下输出表明 3 个资源不符合名为 InstanceTypesAreT2micro 的规则。

输出：

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
```

```
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考[DescribeComplianceByConfigRule](#)中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例检索规则的合规性详细信息，该规则当前没有评估结果 ebs-optimized-instance，因此它返回 INSUFKIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

输出：

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

示例 2：此示例返回规则 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK 的不合规资源数量。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       2
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) [DescribeComplianceByConfigRule](#)中的。

适用于 PowerShell V5 的工具

示例 1：此示例检索规则的合规性详细信息，该规则当前没有评估结果 ebs-optimized-instance，因此它返回 INSUFKIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

输出：

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

示例 2：此示例返回规则 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK 的不合规资源数量。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       2
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeComplianceByConfigRule中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeComplianceByResource** 与 CLI 配合使用

以下代码示例演示如何使用 DescribeComplianceByResource。

CLI

Amazon CLI

获取 Amazon 资源的合规性信息

以下命令返回 Amazon Config 记录的每个违反一条或多条规则的 EC2 实例的合规性信息：

```
aws configservice describe-compliance-by-resource --resource-
type AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

在输出中，每个 CappedCount 属性的值都表示该资源违反了多少规则。例如，以下输出表明实例 i-1a2b3c4d 违反了 2 条规则。

输出：

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DescribeComplianceByResource中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例检查“COMPLIANT”合规类型的 **AWS::SSM::ManagedInstanceInventory** 资源类型。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

输出：

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeComplianceByResource中的。

适用于 PowerShell V5 的工具

示例 1：此示例检查“COMPLIANT”合规类型的 **AWS::SSM::ManagedInstanceInventory** 资源类型。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

输出：

```
Compliance                              ResourceId          ResourceType
----------                              ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeComplianceByResource中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeConfigRuleEvaluationStatus** 与 CLI 配合使用

以下代码示例演示如何使用 DescribeConfigRuleEvaluationStatus。

CLI

Amazon CLI

获取 Amazon Config 规则的状态信息

以下命令返回名为的 Amazon Config 规则的状态信息MyConfigRule：

```
aws configservice describe-config-rule-evaluation-status --config-rule-
names MyConfigRule
```

输出：

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DescribeConfigRuleEvaluationStatus中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例返回给定配置规则的状态信息。

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

输出：

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeConfigRuleEvaluationStatus中的。

适用于 PowerShell V5 的工具

示例 1：此示例返回给定配置规则的状态信息。

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

输出：

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeConfigRuleEvaluationStatus中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeConfigRules`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeConfigRules`。

CLI

Amazon CLI

获取 Amazon Config 规则的详细信息

以下命令返回名为的 Amazon Config 规则的详细信息InstanceTypesAreT2micro：

```
aws configservice describe-config-rules --config-rule-
names InstanceTypesAreT2micro
```

输出：

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DescribeConfigRules中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例列出账户的配置规则以及选定属性。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

输出：

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                  ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                           config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                             config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required      config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeConfigRules中的。

适用于 PowerShell V5 的工具

示例 1：此示例列出账户的配置规则以及选定属性。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

输出：

```
ConfigRuleName                                  ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
```

```
--------------                                      ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                               config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                 config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required          config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeConfigRules中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.
```

```
        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- 有关 API 的详细信息，请参阅适用DescribeConfigRules于 Python 的Amazon SDK (Boto3) API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    DATA(lo_result) = lo_cfs->describeconfigrules(
      it_configrulenames = VALUE /aws1/
cl_cfsconfigrulenames_w=>tt_configrulenames(
        ( NEW /aws1/cl_cfsconfigrulenames_w( iv_rule_name ) )
      )
    ).
    ot_cfg_rules = lo_result->get_configrules( ).
    MESSAGE 'Retrieved AWS Config rule data.' TYPE 'I'.
```

- 有关 API 的详细信息，请参阅适用DescribeConfigRules于 S AP 的Amazon SDK ABAP API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeConfigurationRecorderStatus** 与 CLI 配合使用

以下代码示例演示如何使用 DescribeConfigurationRecorderStatus。

CLI

Amazon CLI

获取配置记录器的状态信息

以下命令返回默认配置记录器的状态。

```
aws configservice describe-configuration-recorder-status
```

输出：

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DescribeConfigurationRecorderStatus中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例返回配置记录器的状态。

```
Get-CFGConfigurationRecorderStatus
```

输出：

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeConfigurationRecorderStatus中的。

适用于 PowerShell V5 的工具

示例 1：此示例返回配置记录器的状态。

```
Get-CFGConfigurationRecorderStatus
```

输出：

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeConfigurationRecorderStatus中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeConfigurationRecorders** 与 CLI 配合使用

以下代码示例演示如何使用 DescribeConfigurationRecorders。

CLI

Amazon CLI

获取有关配置记录器的详细信息

以下命令返回有关默认配置记录器的详细信息：

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

输出：

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DescribeConfigurationRecorders中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例返回配置记录器的详细信息。

```
Get-CFGConfigurationRecorder | Format-List
```

输出：

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeConfigurationRecorders中的。

适用于 PowerShell V5 的工具

示例 1：此示例返回配置记录器的详细信息。

```
Get-CFGConfigurationRecorder | Format-List
```

输出：

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeConfigurationRecorders中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeDeliveryChannels** 与 CLI 配合使用

以下代码示例演示如何使用 DescribeDeliveryChannels。

CLI

Amazon CLI

获取有关传输通道的详细信息

以下命令返回有关传输通道的详细信息：

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

输出：

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考DescribeDeliveryChannels中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例检索该地区的传输通道并显示详细信息。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

输出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) DescribeDeliveryChannels中的。

适用于 PowerShell V5 的工具

示例 1：此示例检索该地区的传输通道并显示详细信息。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

输出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) DescribeDeliveryChannels中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **GetComplianceDetailsByConfigRule** 与 CLI 配合使用

以下代码示例演示如何使用 GetComplianceDetailsByConfigRule。

CLI

Amazon CLI

获取 Amazon Config 规则的评估结果

以下命令返回所有不符合名为的 Amazon Config 规则的资源的评估结果InstanceTypesAreT2micro：

```
aws configservice get-compliance-details-by-config-rule --config-rule-
name InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

输出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
```

```
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考[GetComplianceDetailsByConfigRule](#)中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例获取规则的评估结果 access-keys-rotated并返回按合规类型分组的输出

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

输出：

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

示例 2：此示例查询合规资源的规则 access-keys-rotated的合规性详细信息。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

输出：

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetComplianceDetailsByConfigRule中的。

适用于 PowerShell V5 的工具

示例 1：此示例获取规则的评估结果 access-keys-rotated并返回按合规类型分组的输出

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

输出：

```
Count Name                     Group
----- ----                     -----
    2 COMPLIANT                {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT            {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

示例 2：此示例查询合规资源的规则 access-keys-rotated的合规性详细信息。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

输出：

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetComplianceDetailsByConfigRule中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **GetComplianceDetailsByResource** 与 CLI 配合使用

以下代码示例演示如何使用 `GetComplianceDetailsByResource`。

CLI

Amazon CLI

获取 Amazon 资源的评估结果

以下命令返回 EC2 实例`i-1a2b3c4d`不符合的每条规则的评估结果：

```
aws configservice get-compliance-details-by-resource --resource-
type AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

输出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考GetComplianceDetailsByResource中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例提供给定资源的评估结果。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

输出：

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
ResultToken               :
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetComplianceDetailsByResource中的。

适用于 PowerShell V5 的工具

示例 1：此示例提供给定资源的评估结果。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

输出：

```
Annotation                :
ComplianceType            : COMPLIANT
ConfigRuleInvokedTime     : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime        : 8/25/2019 11:34:56 PM
ResultToken               :
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetComplianceDetailsByResource中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **GetComplianceSummaryByConfigRule** 与 CLI 配合使用

以下代码示例演示如何使用 GetComplianceSummaryByConfigRule。

CLI

Amazon CLI

获取您的 Amazon Config 规则的合规性摘要

以下命令返回合规和不合规的规则数量。

```
aws configservice get-compliance-summary-by-config-rule
```

在输出中，每个 CappedCount 属性的值都表示有多少规则合规或不合规。

输出：

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考GetComplianceSummaryByConfigRule中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例返回不合规的 Config 规则的数量。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       9
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetComplianceSummaryByConfigRule中的。

适用于 PowerShell V5 的工具

示例 1：此示例返回不合规的 Config 规则的数量。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       9
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetComplianceSummaryByConfigRule中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **GetComplianceSummaryByResourceType** 与 CLI 配合使用

以下代码示例演示如何使用 GetComplianceSummaryByResourceType。

CLI

Amazon CLI

获取所有资源类型的合规性摘要

以下命令返回不合规的 Amazon 资源数量和合规资源的数量：

```
aws configservice get-compliance-summary-by-resource-type
```

在输出中，每个 CappedCount 属性的值都表示有多少资源合规或不合规。

输出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

获取特定资源类型的合规性摘要

以下命令返回不合规的 EC2 实例数量和合规的实例数量：

```
aws configservice get-compliance-summary-by-resource-type --resource-
types AWS::EC2::Instance
```

在输出中，每个 CappedCount 属性的值都表示有多少资源合规或不合规。

输出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考[GetComplianceSummaryByResourceType](#)中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例返回合规或不合规资源的数量，并将输出转换为 json。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) GetComplianceSummaryByResourceType中的。

适用于 PowerShell V5 的工具

示例 1：此示例返回合规或不合规资源的数量，并将输出转换为 json。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) GetComplianceSummaryByResourceType中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`PutConfigRule`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `PutConfigRule`。

CLI

Amazon CLI

添加 Amazon 托管 Config 规则

以下命令提供用于添加 Amazon 托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

对于该ComplianceResourceTypes属性，此 JSON 代码将范围限制为该AWS::EC2::Instance类型的资源，因此 Amazon Config 将仅根据规则评估 EC2 实例。由于该规则是托管规则，因此 Owner 属性设置为，AWSSourceIdentifier 属性设置为规则标识符。REQUIRED_TAGS对于 InputParameters 属性，指定了规则所需的标签键 CostCenter 和 Owner。

如果命令成功， Amazon Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules命令并指定规则名称。

添加客户托管的 Config 规则

以下命令提供用于添加客户托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

InstanceTypesAreT2micro.json 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
```

```
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

对于该ComplianceResourceTypes属性，此 JSON 代码将范围限制为该AWS::EC2::Instance类型的资源，因此 Amazon Config 将仅根据规则评估 EC2 实例。由于此规则是客户托管规则，因此该Owner属性设置为CUSTOM_LAMBDA，并且该SourceIdentifier属性设置为 Lambda 函数 Amazon 的 ARN。SourceDetails 对象为必填项。当 Confi Amazon g 调用 Amazon Lambda 函数来根据规则评估资源时，为该InputParameters属性指定的参数将传递给 Lambda 函数。

如果命令成功， Amazon Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules命令并指定规则名称。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考PutConfigRule中的。

Python

适用于 Python 的 SDK（Boto3）

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """
```

```
    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅适用PutConfigRule于 Python 的Amazon SDK (Boto3) API 参考。

SAP ABAP

适用于 SAP ABAP 的 SDK

> **Note**
>
> 还有更多相关信息 GitHub。在 Amazon 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
    " Create a config rule for S3 bucket public read prohibition
    lo_cfs->putconfigrule(
      io_configrule = NEW /aws1/cl_cfsconfigrule(
        iv_configrulename = iv_rule_name
        iv_description = |S3 Public Read Prohibited Bucket Rule|
        io_scope = NEW /aws1/cl_cfsscope(
          it_complianceresourcetypes = VALUE /aws1/
cl_cfscplncresrctypes_w=>tt_complianceresourcetypes(
            ( NEW /aws1/cl_cfscplncresrctypes_w( |AWS::S3::Bucket| ) )
          )
        )
        io_source = NEW /aws1/cl_cfssource(
          iv_owner = |AWS|
          iv_sourceidentifier = |S3_BUCKET_PUBLIC_READ_PROHIBITED|
        )
        iv_inputparameters = '{}'
        iv_configrulestate = |ACTIVE|
      )
    ).
    MESSAGE 'Created AWS Config rule.' TYPE 'I'.
```

- 有关 API 的详细信息，请参阅适用PutConfigRule于 S AP 的Amazon SDK ABAP API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **PutDeliveryChannel** 与 CLI 配合使用

以下代码示例演示如何使用 PutDeliveryChannel。

CLI

Amazon CLI

创建传输通道

以下命令以 JSON 代码的形式提供传输通道的设置：

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

deliveryChannel.json 文件指定了传输通道的属性：

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

此示例设置了以下属性：

name——传输通道的名称。默认情况下，Amazon Config 会default将名称分配给新的交付渠道。您无法使用命令更新传递渠道名称。put-delivery-channel有关更改名称的步骤，请参阅“重命名传输通道”。s3BucketName- Amazon Config 向其发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另一个 Amazon 账户，则该存储桶必须具有授予对 Config Amazon 的访问权限的策略。有关更多信息，请参阅 Amazon S3 存储桶的权限。

snsTopicARN-Amazon SNS 主题的亚马逊资源名称 (ARN)，Amazon Config 会向该主题发送有关配置变更的通知。如果您从其他账户选择主题，则该主题必须具有授予对 Config 的访问权限的策略。 Amazon 有关更多信息，请参阅 Amazon SNS 主题的权限。

configSnapshotDeliveryProperties-包含deliveryFrequency属性，该属性设置 Amazon Config 提供配置快照的频率以及它为定期 Config 规则调用评估的频率。

如果命令成功，Amazon Config 将不返回任何输出。要验证您的配送渠道的设置，请运行 describe-delivery-channels命令。

- 有关 API 的详细信息，请参阅Amazon CLI 命令参考PutDeliveryChannel中的。

PowerShell

适用于 PowerShell V4 的工具

示例 1：此示例更改现有传输通道的 deliveryFrequency 属性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 4) PutDeliveryChannel中的。

适用于 PowerShell V5 的工具

示例 1：此示例更改现有传输通道的 deliveryFrequency 属性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 amzn-s3-demo-bucket -DeliveryChannel_S3KeyPrefix my
```

- 有关 API 的详细信息，请参阅 Amazon Tools for PowerShell Cmdlet 参考 (V 5) PutDeliveryChannel中的。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Config与Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

文档历史记录

下表描述了对的文档所做的重要更改 Amazon Config。要获得本文档的更新通知，您可以订阅 RSS 源。

- API 版本：2014-11-12
- 最新文档更新：2026 年 1 月 9 日

变更	说明	日期
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • cloudformation-stack-service-role-检查 • cloudfront-distribution-key-group-已启用 • ecs-capacity-provider-termination-检查 • ecs-task-definition-linux-user-non-root • ecs-task-definition-windows-user-non-admin	2026年1月9日
Amazon Config 支持 S3 表所需的新权限	在此版本 Amazon Config 中，添加了记录 S3 Tables 资源类型所需的新权限。有关更多信息，请参阅支持的资源类型。	2026年1月9日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • aurora-global-database-encryption-在休息时 • cloudformation-termination-protection-check	2025 年 12 月 8 日

	• cognito-userpool-cust-auth-threat-full-check • cognito-user-pool-deletion-已启用保护 • cognito-user-pool-mfa-已启用 • ebs-snapshot-block-public-访问 • ecs-task-definition-efs-已启用加密 • ses-sending-tls-required	
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • aurora-global-database-encryption-在休息时 • cloudformation-termination-protection-check • cognito-userpool-cust-auth-threat-full-check • cognito-user-pool-deletion-已启用保护 • cognito-user-pool-mfa-已启用 • ebs-snapshot-block-public-访问 • ecs-task-definition-efs-已启用加密 • ses-sending-tls-required	2025 年 12 月 8 日

???	示例跨账户 S3 存储桶策略不再包括`config.amazonaws.com` 服务主体。有关更多信息，请参阅required-permissions-cross-account。	2025年12月3日
安全 IAM 更新	`AWSConfigServiceRolePolicy` 和`AWS_ConfigRole` 政策现在为亚马逊 Lightsail 和亚马逊简单存储服务 (Amazon S3) Service 授予额外权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2025 年 11 月 20 日
安全 IAM 更新	Amazon Config 更新了托管策略`AWSConfigServiceRolePolicy` ，增强了针对 100 多项 Amazon 服务的 Amazon 资源配置记录的全面权限的文档。有关信息，请参阅Amazon 托管策略的Amazon Config 更新。	2025 年 11 月 11 日
安全 IAM 更新	Amazon Config 已更新托管策略`AWS_ConfigRole` ，使其具有跨多个服务记录 Amazon 资源配置的全面权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2025 年 11 月 10 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • amplify-app-no-environment-变量 • amplify-branch-description • api-gwv2--启用指标 stage-default-route-detailed • apigateway-stage-description • apigatewayv2-stage-description • appconfig-deployment-strategy-tagged • aps-rule-groups-namespace-已标记 • auditmanager-assessment-tagged • batch-managed-spot-compute-environment-max-bid • cognito-identity-pool-unauthenticated-登录 • customerprofiles-domain-tagged • devicefarm-project-tagged • devicefarm-test-grid-project-已标记 • ec2-network-insights-analysis-tagged • eks-fargate-profile-tagged • glue-ml-transform-tagged	2025 年 10 月 27 日

	• iot-provisioning-template-description • iot-provisioning-template-jitp • iot-provisioning-template-tagged • iot-scheduled-audit-tagged • kinesis-video-stream-minimum-数据保留 • lambda-function-description • lightsail-bucket-allow-public-重写-已禁用 • route53--已标记 resolver-firewall-domain-list • route53-协会已标记 resolver-firewall-rule-group • route53--已标记 resolver-firewall-rule-group • 53 号公路-resolver-resolver-rule-tagged • rum-app-monitor-cloudwatch-启用日志 • rum-app-monitor-tagged	
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新 Amazon API Gateway 和 Amazon Config 资源类型的配置更改。 Amazon CloudTrail 有关更多信息，请参阅支持的资源类型。	2025 年 10 月 10 日

Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包：亚马逊 S3、亚马逊 EBS 和亚马逊 DynamoDB 的网络弹性最佳实践	2025 年 10 月 3 日
安全 IAM 更新	`AWSConfigServiceRolePolicy` 和`AWS_ConfigRole` 政策现在为、、、Amazon Bedrock Amazon Amplify、、、、 Amazon AppSync、、Amazon Connect、 Amazon CloudTrail、 Amazon CloudFormation、亚马逊 Amazon CodeArtifact、、 Amazon CodePipeline、、亚马逊、 Amazon Deadline Cloud、Amazon Quick Suite EC2 Amazon Entity Resolution 数据匹配服务 Amazon IoT SiteWise、Amazon Redshift、 Amazon Lambda Serverless、、、、Amazon Security Lak Amazon Service Catalog e Amazon Identity and Access Management Roles Anywhere、、、、Amazon Systems Manager Amazon Secrets Manager、、、Amazon Systems Manager 和。 EventBridge SageMaker Amazon Shield EC2 Amazon WAFV2有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2025 年 10 月 1 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • cognito-user-pool-password-政策检查 • dms-replication-instance-multi-az 已启用 • ec2-已加launch-templates-ebs-volume密 • rds-mysql-cluster-copy-tags-to-snapshot-check • rds-pgsql-cluster-copy-tags-to-snapshot-check	2025 年 10 月 1 日
Amazon Config 支持亚太地区（台北）区域的新资源类型	在此版本中，Amazon Config 现在支持亚太地区（台北）区域的以下 Amazon WAFV2 资源类型： • AWS:WAFv2::: IPSet • AWS::WAFv2::ManagedRuleSet • AWS::WAFv2::RegexPatternSet • AWS::WAFv2::RuleGroup • AWS::WAFv2::WebACL 有关更多信息，请参阅按区域可用性列出的资源覆盖范围。	2025 年 9 月 23 日

Amazon Config 更新一致性包	在此版本中，更新 Amazon Config 了以下一致性包： • ACSC Essential 8 操作最佳实践 • ACSC ISM 操作最佳实践 - 第 2 部分	2025 年 9 月 9 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新 Amazon CodeArtifact、Amazon Config Amazon Glue Amazon Network Manager、和 Amazon Identity and Access Management 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2025 年 9 月 3 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的、亚马逊 OpenSearch 服务、亚马逊 Amazon Backup、适用于 Apache Managed Streaming Kafka EC2、Amazon Redshift、Route 53 Profiles、 Amazon Systems Manager Incident Manager、 Amazon Transfer Family、和亚马逊资源类型的配置更改。 CloudFront 有关更多信息，请参阅支持的资源类型。	2025 年 8 月 15 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • cloudfront-origin-lambda-url-oac已启用 • sqs-queue-policy-full-访问检查 • sqs-queue-dlq-check	2025 年 8 月 14 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • alb-tagged • api-gw-rest-api-已标记 • api-gw-stage-tagged • appsync-graphql-api-xray-已启用 • cloudwatch-metric-stream-tagged • codebuild-report-group-tagged • datasync-location-object-storage-使用-https • ec2-vpn-connection-tagged • ecs-capacity-provider-tagged • efs-file-system-tagged • eks-addon-tagged • elb-internal-scheme-check • elb-tagged • glb-tagged • iot-job-template-tagged • iotdevicedefender-custom-metric-tagged • kms-key-tagged • msk-cluster-tagged • nlb-tagged • rds-event-subscription-tagged • rds-option-group-tagged	2025 年 8 月 13 日

- 53 号公路-health-check-tagged
- 53 号公路-hosted-zone-tagged
- service-catalog-portfolio-tagged
- stepfunctions-state-machine-tagged
- workspaces-connection-alias-tagged
- workspaces-workspace-tagged

安全 IAM 更新	该AWS_ConfigRole 政策现在为亚马逊 Bedrock Amazon ARC - Zonal Shift、、、、、、 Amazon CloudTrail、 Amazon CodeArtifact、Amazon Deadline Cloud、Amazon Database Migration Service Amazon Glue Amazon Identity and Access Management、Amazon Managed Streaming Amazon Lake Formation、、、、A CloudWatch mazon AWS Elemental MediaLive Logs AWS Elemental MediaPackage、、、、亚马逊关系数据库服务、亚马逊简单存储服务 Amazon Secrets Manager、、亚马逊安全湖 Amazon Service Catalog、、亚马逊简单电子邮件服务和。 Amazon X-Ray 有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2025 年 7 月 28 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策现在为亚马逊 Bedrock Amazon ARC - Zonal Shift、、、、、、、Amazon CloudTrail Amazon CodeArtifact Amazon Deadline Cloud Amazon Database Migration Service Amazon Glue、Amazon Managed Kafka Amazon Identity and Access Management、Amazon Lake Formation 、、、、、、、 CloudWatch Amazon L AWS Elemental MediaLive ogs AWS Elemental MediaPackage、、、、、亚马逊关系数据库服务、亚马逊简单存储服务 Amazon Secrets Manager、亚马逊安全湖 Amazon Service Catalog、亚马逊简单电子邮件 Amazon X-Ray服务和亚马逊 API Gateway 授予额外权限。有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2025 年 7 月 28 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的、、、、Amazon Amazon Backup、、、 Amazon 账单与成本管理 Amazon CloudFormation CloudFront Amazon Entity Resolution 数据匹配服务 Amazon IoT、 Amazon 私有证书颁发机构 Amazon Relational Database Service 和 Amazon S3 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2025 年 7 月 15 日
安全 IAM 更新	现在，该AWS_ConfigRole 策略和AWSConfigServiceRolePolicy 政策为、、Amazon Bedrock Amazon Backup gateway、、Amazon 账单与成本管理、Amazon、、、、、 Amazon CloudFormation CloudFront、Amazon Redshift Amazon Entity Resolution 数据匹配服务 Amazon IoT Core Device Advisor Amazon Lambda Amazon Network Manager Amazon 私有证书颁发机构、Amazon S3 Tables 等授予额外权限。 Amazon Systems Manager 快速设置功能有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2025 年 6 月 18 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新 Amazon Bedrock 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2025 年 6 月 17 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • cloudfront-ssl-policy-check • cognito-identity-pool-unauth-访问检查 • ec2-已enis-source-destination-check启用 • elbv2-listener-encryption-in-transit • lambda-function-xray-enabled • msk-cluster-public-access-已禁用 • msk-connect-connector-logging-已启用 • msk-unrestricted-access-check • aurora-mysql-cluster-audit-日志 • redshift-cluster-multi-az-已启用 • s3 express-dir-bucket-lifecycle-规则检查 • ssm-automation-logging-enabled • ssm-automation-block-public-共享	2025 年 6 月 13 日

安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略和 `AWS_ConfigRole` 策略现在为 Amazon Bedrock 授予更多权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2025 年 5 月 27 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的亚马逊应用程序集成、亚马逊弹性计算云（亚马逊 EC2）、Amazon Inspector、Amazon Macie、亚马逊 Route 53 Profiles、Amazon Serverless、亚马逊简单存储服务 (A OpenSearch mazon S3) Serverless、亚马逊简单存储服务 (Amazon S Amazon Security Hub CSPM 3) 和亚马逊 AI 资源类型的配置更改。SageMaker 有关更多信息，请参阅支持的资源类型。	2025 年 4 月 30 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则：redshift-serverless-default-db-name-check	2025 年 4 月 22 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则：redshift-serverless-default-admin-check	2025 年 4 月 17 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在授予了以下方面的额外权限：Amazon Bedrock、、、 Amazon Clean Rooms、Amazon Database Migration Service （Amazon DMS ）Amazon CodeConnections Amazon Direct Connect、Amazon L CloudWatch ogs、Amazon Macie、亚马逊托管区块链、亚马逊 Q Business、Route 53 个人资料、亚马逊简单存储服务 (Amazon S3)、A SageMaker mazon AI Amazon Security Hub CSPM、 Amazon Systems Manager Incident Manager以及联系人和。Amazon B2B Data Interchange Amazon Systems Manager Incident Manager Amazon Systems Manager有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2025 年 4 月 8 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • s3-bucket-tagged • ecr-repository-tagged • sagemaker-feature-group-tagged • sagemaker-domain-tagged • cognito-user-pool-tagged	2025 年 4 月 1 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • nlb-cross-zone-load-启用平衡 • redshift-serverless-publish-logs到云端观察 • rds-instance-subnet-igw-检查 • ec2-spot-fleet-request-ct-encryption-at-rest • redshift-serverless-workgroup-encrypted在途中 • redshift-serverless-workgroup-no-公共访问 • redshift-serverless-namespace-cmk-加密 • event-data-store-cmk-已启用加密 • ecs-task-definition-network-mode-not-host • rds-proxy-tls-encryption • nlb-logging-enabled • redshift-audit-logging-enabled • s3-lifecycle-policy-check • sagemaker-image-tagged • redshift-cluster-parameter-group-已标记 • ec2-dhcp-options-tagged • sagemaker-app-image-config-已标记	2025 年 3 月 22 日

- mariadb-publish-logs-to-云监视日志
- docdb-cluster-encrypted-in-交通
- rds-sqlserver-encrypted-in-交通
- ec2-traffic-mirror-session-tagged
- ec2-launch-template-tagged
- ec2-traffic-mirror-target-tagged
- transfer-certificate-tagged
- batch-managed-compute-env-compute-resources-tagged
- lightsail-disk-tagged
- transfer-profile-tagged
- amplify-app-tagged
- ec2-prefix-list-tagged
- amplify-branch-tagged
- transfer-agreement-tagged
- datasync-task-tagged
- transfer-workflow-tagged
- sagemaker_notebook_instance_platform_version
- ec2-traffic-mirror-filter-tagged
- aurora-mysql-cluster-audit-日志
- ssm-document-tagged
- transfer-connector-tagged

- rds-mariadb-instance-encrypted在途中
- iam-saml-provider-tagged
- ec2-fleet-tagged
- iam-server-certificate-tagged
- iam-oidc-provider-tagged
- alb-listener-tagged
- glb-listener-tagged
- ec2-已network-insights-access-scope标记
- lightsail-certificate-tagged
- ec2-capacity-reservation-tagged
- ec2-已transit-gateway-multicast-domain标记
- dms-endpoint-tagged
- ec2-carrier-gateway-tagged
- dms-replication-task-tagged
- ec2-client-vpn-endpoint-tagged
- lightsail-bucket-tagged
- ec2-分析已network-insights-access-scope标记
- nlb-listener-tagged
- ec2-network-insights-path-tagged

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • docdb-cluster-encrypted-in-交通 • mariadb-publish-logs-to-云监视日志 • aurora-mysql-cluster-audit-记录 • rds-mariadb-instance-encrypted在途中 • rds-sqlserver-encrypted-in-交通 • sagemaker-notebook-instance-platform-版本 • appstream-fleet-multi-az • apprunner-vpc-connector-multi-az • mq-broker-general-logging-已启用 • mq-active-single-instance-broker-storage-type-efs • mq-active-broker-ldap-认证 • iottwinmaker-component-type-tagged	2025 年 3 月 19 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • fsx-openzfs-deployment-type-检查 • fsx-ontap-deployment-type-检查 • fsx-windows-deployment-type-检查 • redshift-serverless-workgroup-routes-在 vpc 内	2025 年 3 月 18 日
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则：ec2-instance-launched-with-allowed-ami	2025 年 3 月 11 日

Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • connect-instance-logging-enabled • ecr-repository-cmk-encryption-已启用 • elbv2--check predefined-security-policy-ssl • glue-spark-job-supported-版本 • guardduty-runtime-monitoring-enabled • guardduty-ecs-protection-runtime-已启用 • guardduty-ec2-protection-runtime-enabled • netfw-subnet-change-protection-已启用 • rds-sql-server-logs到云端观察 • sqs-queue-no-public-访问 • transfer-connector-logging-enabled	2025 年 3 月 7 日
安全 IAM 更新	现在，该`AWSConfig ServiceRolePolicy` 策略和`AWS_ConfigRole` 策略授予亚马逊弹性计算云 (Amazon EC2) 的额外权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2025 年 3 月 4 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • athena-workgroup-description • amplify-app-tagged • sagemaker-app-image-config-已标记 • elasticbeanstalk-application-version-description • amplify-branch-performance-mode-已启用 • athena-workgroup-engine-version-自动升级 • sagemaker-image-description • devicefarm-instance-profile-tagged • transfer-workflow-description • ec2-traffic-mirror-session-tagged • appstream-fleet-in-vpc • transfer-agreement-tagged • ec2-traffic-mirror-target-description • transfer-agreement-description • athena-prepared-statement-description • batch-managed-compute-env-compute-resources-tagged	2025 年 2 月 8 日

- codedeploy-deployment-group-auto-启用回滚
- batch-managed-compute-environment-using-launch-template
- ec2-prefix-list-tagged
- ec2-traffic-mirror-filter-tagged
- athena-workgroup-enforce-workgroup-配置
- transfer-certificate-tagged
- batch-compute-environment-managed
- lightsail-disk-tagged
- transfer-profile-tagged
- ec2-traffic-mirror-target-tagged
- appintegrations-event-integration-tagged
- datasync-task-tagged
- batch-compute-environment-enabled
- appconfig-configuration-profile-validators-不为空
- elasticbeanstalk-application-description
- codedeploy-deployment-group-outdated-实例更新
- ec2-launch-template-tagged
- fis-experiment-template-tagged
- ivs-channel-playback-authorization-已启用

- redshift-cluster-parameter-group-已标记
- ec2-traffic-mirror-filter-description
- appintegrations-event-integration-description
- athena-data-catalog-description
- fis-experiment-template-log-配置-存在
- amplify-app-description
- amplify-branch-tagged
- batch-job-queue-enabled
- elasticbeanstalk-environment-description
- amplify-app-branch-auto-已启用删除
- appconfig-hosted-configuration-version-描述
- appconfig-freeform-profile-config-存储
- datasync-task-data-verification-已启用
- apprunner-service-observability-enabled
- transfer-certificate-description
- appconfig-deployment-strategy-replicateto-ssm
- transfer-workflow-tagged
- transfer-connector-tagged
- ec2-traffic-mirror-session-description

	• customerprofiles-object-type-allow-创建个人资料 • sagemaker-image-tagged	
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的亚马逊简单存储服务 (Amazon S3) Service 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2025 年 2 月 6 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的亚马逊简单存储服务 (Amazon S3) Service 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2025 年 1 月 29 日
安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊 Comprehend Amazon Clean Rooms、亚马逊弹性计算云 EC2（亚马逊）、亚马逊简单存储服务（Amazon S3 Amazon HealthOmics）和亚马逊简单电子邮件服务（Amazon SES）和亚马逊简单电子邮件服务（Amazon SES）授予额外权限。有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2025 年 1 月 16 日

Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • appmesh-mesh-deny-tcp-转发 • sagemaker-model-isolation-enabled • evidently-project-description • alb-internal-scheme-check • evidently-segment-description • appconfig-environment-description • apprunner-service-in-vpc • sagemaker-domain-in-vpc • nlb-internal-scheme-check • emr-security-configuration-encryption-休息 • apprunner-service-no-public-访问 • sagemaker-model-in-vpc • appconfig-deployment-strategy-description • evidently-launch-description • iot-authorizer-token-signing-已启用	2025 年 1 月 9 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的亚马逊弹性计算云 (Amazon EC2) 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2025 年 1 月 9 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • batch-job-queue-tagged • iottwinmaker-sync-job-tagged • codeguruprofiler-profiling-group-tagged • ivs-recording-configuration-tagged • iottwinmaker-entity-tagged • iottwinmaker-workspace-tagged • iottwinmaker-scene-tagged • acmpca-certificate-authority-tagged • appflow-flow-tagged • iotevents-detector-model-tagged • appmesh-virtual-node-logging-file-path-exists • apprunner-vpc-connector-tagged • apprunner-service-tagged • iotwireless-fuota-task-tagged • appmesh-virtual-node-backend-defaults-tls-on • codegurureviewer-repository-association-tagged • iotevents-input-tagged • appmesh-virtual-gateway-logging-file-path-exists	2025 年 1 月 8 日

	• batch-compute-environment-tagged • batch-scheduling-policy-tagged • customerprofiles-object-type-tagged • emr-security-configuration-encryption-交通 • iotwireless-service-profile-tagged • ivs-playback-key-pair-已标记 • cassandra-keyspace-tagged • iotevents-alarm-model-tagged • appconfig-application-description • appmesh-virtual-gateway-backend-默认值-tls • ivs-channel-tagged • iotwireless-multicast-group-tagged	
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的亚马逊弹性计算云 (Amazon EC2)、Amazon Cognito 和亚马逊 OpenSearch 服务资源类型的配置更改。 AWS Elemental MediaConnect有关更多信息，请参阅支持的资源类型。	2024 年 12 月 19 日

安全 IAM 更新	现在，该AWSConfig ServiceRolePolicy 策略为授予了额外的权限 Amazon Organizations。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2024 年 12 月 18 日
Amazon Config 支持与服务相关的配置记录器	在此版本中， Amazon Config 支持与服务相关的配置记录器。您可以在支持的服务中或使用启用与服务相关的配置记录器 Amazon CLI，该记录器将代表您记录关联服务所需的资源类型。您可以使用 Amazon Config 控制台或 Amazon CLI查看与服务相关的配置记录器的详细信息。有关更多信息，请参阅使用配置记录器。	2024 年 11 月 27 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • appconfig-application-tagged • appconfig-configuration-profile-tagged • appconfig-environment-tagged • appconfig-extension-association-tagged • appmesh-gateway-route-tagged • appmesh-mesh-tagged • appmesh-route-tagged • appmesh-virtual-gateway-tagged • appmesh-virtual-node-tagged • appmesh-virtual-router-tagged • appmesh-virtual-service-tagged • evidently-launch-tagged • evidently-project-tagged • evidently-segment-tagged • frauddetector-entity-type-tagged • frauddetector-label-tagged • frauddetector-outcome-tagged • frauddetector-variable-tagged	2024 年 11 月 12 日

	• iotsitewise-asset-model-tagged • iotsitewise-dashboard-tagged • iotsitewise-gateway-tagged • iotsitewise-portal-tagged • iotsitewise-project-tagged	
安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为、、Amazon Connect、Amazon Amazon AppConfig Amazon CloudTrail、Amazon DevOps Guru DataZone、、Identity Store、 Amazon Glue、、、亚马逊互动视频服务 (Amazon IVS) Amazon IoT FleetWise Amazon IoT Wireless、亚马逊 CloudWatch 日志、亚马逊可观察性访问管理器、亚马逊关系 Amazon Payment Cryptography数据库服务 (Amazon RDS)、Ama CloudWatch zon Rekognition、亚马逊简单存储服务 (Amazon S3) 授予额外权限) Simple Service、Amazon Scheduler 和 Amazon VPC Lattice。 Amazon IoT EventBridge Amazon Systems Manager有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2024 年 11 月 8 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则：cognito-user-pool-advanced-启用安全	2024 年 11 月 6 日
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • active-mq-supported-version • rabbit-mq-supported-version • ec2-vpn-connection-logging-enabled • appsync-cache-ct-encryption-在休息时 • appsync-cache-ct-encryption在途中 • vpc-endpoint-enabled • efs-filesystem-ct-encrypted • redshift-cluster-subnet-group-多可用区 • sns-topic-no-public-访问 • rabbit-mq-supported-version • kms-key-policy-no-公共访问 • rds-mysql-instance-encrypted在途中 • rds-postgres-instance-encrypted在途中 • rds-sql-server-logs到云端观察 • ec launch-template-imdsv2-2-check	2024 年 10 月 21 日

Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包： • PCI DSS 4.0 操作最佳实践（不包括全局资源类型） • PCI DSS 4.0 操作最佳实践（包括全局资源类型）	2024 年 9 月 23 日
安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊 OpenSearch 服务 Severless、、、、、、Im EC2 age Builder AppStream 、 Amazon Backup、Amazon CloudTrail Amazon Glue、Amazon Interactive Video Service Amazon IoT、、、 AWS Elemental MediaConnect AWS Elemental MediaTailor、 Amazon HealthOmics和 Amazon Scheduler 授予额外权限。EventBridge 有关更多信息，请参阅适用于 Amazon Config的 Amazon 托管策略。	2024 年 9 月 16 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • ec2-resources-in-logically-air-gapped-vault • ebs-resources-in-logically-air-gapped-vault • aurora-resources-in-logically-air-gapped-vault • efs-resources-in-logically-air-gapped-vault • s3-resources-in-logically-air-gapped-vault • storagegateway-resources-in-logically-air-gapped-vault • virtualmachine-resources-in-logically-air-gapped-vault	2024 年 9 月 3 日
Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包： • FedRAMP 操作最佳实践（高级部分 1） • FedRAMP 操作最佳实践（高级部分 2）	2024 年 8 月 27 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • athena-workgroup-logging-enabled • codebuild-report-group-encrypted-在休息时 • cognito-user-pool-advanced-已启用安全性 • datasync-task-logging-enabled • efs-automatic-backups-enabled • glue-job-logging-enabled • glue-ml-transform-encrypted-在休息时 • kinesis-stream-backup-retention-检查 • rds-aurora-postgresql-logs到云端观察 • rds-postgresql-logs-to-云观察 • workspaces-root-volume-encryption-已启用 • workspaces-user-volume-encryption-已启用	2024 年 7 月 22 日

安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略和 `AWS_ConfigRole` 策略现在为 Amazon Elastic File System（Amazon EFS）、Amazon Redshift 和 适用于 SAP 的 Amazon Systems Manager授权更多权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2024 年 6 月 17 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • cloudtrail-s3-bucket-public-access-prohibited • cloudtrail-s3-bucket-access-logging	2024 年 5 月 8 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则：iam-external-access-analyzer- enabled	2024 年 5 月 2 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • guardduty-malware-protection-enabled • guardduty-rds-protection-enabled • guardduty-s3-protection-enabled • inspector-lambda-standard-scan-已启用	2024 年 4 月 26 日

Amazon Config 通过 Amazon 简化使用情况分析 CloudWatch	在此版本中，用于监控 Amazon Config 数据使用情况的 Amazon CloudWatch 指标将仅显示可计费的使用量。这意味着，向控制台发送的 Amazon CloudWatch 指标中将不再显示不可计费的使用量。 Amazon Config Amazon Config 这使您可以使用 Amazon CloudWatch 指标验证 Amazon Config 设置和使用情况，并将计费用量与相关费用关联起来。有关更多信息，请参阅 Amazon Config 使用情况和成功指标。	2024 年 4 月 26 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则：iam-server-certificate-expiration- check	2024 年 4 月 23 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • vpc-sg-port-restriction-检查 • cloudtrail-all-write-s3-data-event-check • cloudtrail-all-read-s3-data-event-check	2024 年 4 月 17 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • guardduty-eks-protection-audit-已启用 • guardduty-eks-protection-runtime-已启用 • guardduty-lambda-protection-enabled • inspector-ec2-scan-enabled • inspector-ecr-scan-enabled • inspector-lambda-code-scan-已启用 • redshift-unrestricted-port-access	2024 年 4 月 16 日
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则：efs-mount-target-public- accessible	2024 年 3 月 20 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • dms-neptune-iam-authorization-已启用 • dms-mongo-db-authentication-已启用 • dms-redis-tls-enabled • dax-tls-endpoint-encryption • eks-cluster-secrets-encrypted • kinesis-firehose-delivery-stream-已加密 • mq-cloudwatch-audit-log-已启用 • mq-cloudwatch-audit-log-已启用 • opensearch-primary-node-fault-容忍 • sagemaker-endpoint-config-prod-实例计数 • service-catalog-shared-within-组织 • transfer-family-server-no-ftp	2024 年 2 月 26 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为Prometheus、亚马逊、Amazon Cognito、亚马逊、亚马逊、（IAM）、、、、Amazon Redshift Serverless CloudWatch、Amazon AI 和 ElastiCache亚马逊简单通知服务 (Ama FSx zon SN Amazon Glue S Amazon Identity and Access Management) Simple Notificati Amazon RAM on Serverless Amazon Lambda、Amazon AI 和亚马逊简单通知服务（SageMaker Amazon SNS) 授予额外权限。有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2024 年 2 月 22 日
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则：s3-bucket-cross-region-replication 启用	2024 年 2 月 12 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的、Amazon CloudWatch Evicently、 Amazon Identity and Access Management (IAM) Amazon AppConfig 、Amazon MemoryDB (MemoryDB)、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）、亚马逊 Redshift 和资源类型的配置更改。 Amazon Transfer Family 有关更多信息，请参阅支持的资源类型。	2024 年 2 月 6 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则：macie-auto-sensitive-data-discovery-check	2024 年 1 月 29 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新亚马逊 AppStream、()、亚马逊关系数据库服务 Amazon Key Management Service (Amazon RDS Amazon KMS)、亚马逊 Cognito、亚马逊弹性计算云 (亚马逊)、 EC2 Image Builder、、、、Amazon EC2 Quick Suite Amazon Ground Station、 Amazon Mainframe Modernization Amazon Redshift 和资源类型的配置更改。 Amazon Systems Manager 有关更多信息，请参阅支持的资源类型。	2024 年 1 月 3 日

根据每个账户每个区域的最大 Amazon Config 规则数，服务限制会提高	在此版本中，每个账户 Amazon Config 支持每个 Amazon 区域的 1000 Amazon Config 条规则。这一增长适用于所有已部署规则的总数，包括每个账户每个区域的 Amazon Config 托管规则、 Amazon Config 自定义规则、 Amazon Config 一致性包、 Amazon Security Hub CSPM 控件、 Amazon Firewall Manager 策略和 Amazon Backup 备份计划。有关更多信息，请参阅服务限制。	2023 年 12 月 19 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • s3-meets-restore-time-target • ebs-meets-restore-time-目标 • ec2-meets-restore-time-target • rds-meets-restore-time-目标 • efs-meets-restore-time-目标 • fsx-meets-restore-time-目标 • aurora-meets-restore-time-目标 • dynamodb-meets-restore-time-目标	2023 年 12 月 19 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为适用于 Prometheus 的亚马逊托管服务 Amazon AppConfig、()、Amazon DMS() IAM Amazon Database Migration Service 、适用于 Apache Kafka 的亚马逊托管流媒体（Amazon Identity and Access Management亚马逊 MSK）、亚马逊 Amazon Organizations日志和亚马逊简单存储服务 (Ama CloudWatch zon S3) 授予额外权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2023 年 12 月 5 日
预览版：适用于高级查询的自然语言查询处理器	在此版本中，您可以使用自然语言查询处理器进行高级查询，该处理器使用生成式人工智能（生成人工智能）功能，允许您用通俗易懂的英语提问并将其转换为 ready-to-use 查询格式。使用自然语言查询处理器，您可以对您的组织 Amazon Web Services 账户 或整个 Amazon 组织进行查询。有关更多信息，请参阅适用于高级查询的自然语言查询处理器。	2023 年 11 月 26 日

定期记录	在此版本中，Amazon Config 支持定期录制。定期记录让您能够捕获固定时间段内资源的最新配置更改。现在，您可以将配置记录器的默认频率设置为“每日”，这样您将能够收到代表过去 24 小时内资源的最新状态的配置项（CI），前提是它与之前记录的 CI 不同。Amazon Config 控制台还引入了全新的录制策略体验，您还可以在其中覆盖特定资源类型的录制频率或将特定资源类型排除在录制范围之外。这有助于您的设置符合精细要求。 将添加以下数据类型： • RecordingMode • RecordingModeOverride 将更新以下数据类型： • PutConfigurationRecorder • ConfigurationRecorder • BaseConfigurationItem • ConfigurationItem 将更新开发人员指南中的以下页面： • 对 Amazon 资源重新编码 • 使用 Amazon Config 控制台 Amazon Config 进行设置 | 一键设置	2023 年 11 月 26 日

- 使用 Amazon Config 控制台 Amazon Config 进行设置 | 手动设置
- 使用 Amazon CLI Amazon Config 进行设置

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊 Cognito、Amazon Connect、亚马逊 EMR、、、Amazon MemoryDB、 Amazon Ground Station、 Amazon Mainframe Modernization Amazon Quick Suite Amazon Organizations、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Redshift、Amazon Route 53 和授予额外权限。 Amazon Service Catalog Amazon Transfer Family 现在，AWSConfigServiceRolePolicy 策略和 AWS_ConfigRole 策略还为、AWSConfigServiceRolePolicyStatementID AWSConfigSLRLogStatementID 、AWSConfigSLREventStatementID 、AWSConfigSLRApiGatewayStatementID 和 AWSConfigServiceRolePolicy 策略添加了安全标识符（SID）。 有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2023 年 11 月 17 日

Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • acm-pca-root-ca-已禁用 • dynamodb-table-deletion-protection-已启用 • ec2-已client-vpn-connection-log启用 • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-已配置 • fsx-openzfs-copy-tags-已启用 • fsx-lustre-copy-tags到备份 • msk-enhanced-monitoring-enabled • mq-auto-minor-version-已启用升级 • neptune-cluster-multi-az-已启用 • opensearch-update-check • 仅限 s3 access-point-in-vpc- • s3 access-point-public-access-方块 • s3-bucket-mfa-delete-enabled	2023 年 11 月 9 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的 Amazon Identity and Access Management (IAM)、()、、Amazon Connect Amazon Network Manager、亚马逊弹性计算云 Amazon 私有证书颁发机构 (亚马逊Amazon 私有 CA)、亚马逊弹性容器服务 (亚马逊 ECS EC2)、、、适用于 Apache Kafka Streaming 的亚马逊托管流媒体（亚马逊 MSK Connect） Amazon IoT和资源类型的配置更改。Amazon App Mesh Amazon IoT TwinMaker Amazon Lambda Amazon 资源探索器有关更多信息，请参阅支持的资源类型。	2023 年 11 月 3 日
Amazon Config 支持新的一致性包	在此版本中， Amazon Config 更新了以下一致性包：BN RMi M T 的运营最佳实践	2023 年 10 月 26 日

聚合器的合规性和清单控制面板	在此版本中，在控制台的聚合视图中 Amazon Config 添加了合规性控制面板页面和库存 Amazon Config 控制面板页面。 在合规性控制面板页面中，您可以查看带有小组件的自动控制面板，这些小组件总结了对聚合器中资源合规性的见解，例如按不合规资源列出的排名前 10 的资源类型，按不合规规则列出的排名前 10 的账户级别合规包等。 在清单控制面板页面中，您可以查看带有小组件的自动控制面板，这些小组件总结了对聚合器中资源配置数据的见解，例如按资源计数列出的排名前 10 的资源类型，按资源计数列出的排名前 10 的账户等。 有关图表的信息，请参阅合规性控制面板和清单控制面板。	2023 年 10 月 23 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为、、Amazon Connect Amazon 私有 CA Amazon App Mesh、亚马逊弹性容器服务 (Amazon ECS)、Amazon Evicently、Amazon Managed Grafana、 CloudWatch 亚马逊、Amazon Insp Amazon IoT TwinMaker ector、、、、、 GuardDuty Amazon Apache Kafka Managed Streaming（ Amazon IoT亚马逊 MSK ）、、、和亚马逊人工智能授予额外权限。 Amazon Lambda Amazon Network Manager Amazon Organizations SageMaker 有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2023 年 10 月 4 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新 Amazon IoT的、、、Amazon Personalize Amazon Managed Streaming for Apache Kafka（亚马逊 MSK）SageMaker 、Amazon A Amazon CodeBuild I、Amazon、Amazon 和 Amazon Inspector 资源类型的配置更改。 Amazon IoT TwinMaker Amazon IoT Wireless AppStream有关更多信息，请参阅支持的资源类型。	2023 年 10 月 4 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • docdb-cluster-deletion-protection-已启用 • docdb-cluster-audit-logging-已启用 • docdb-cluster-snapshot-public-禁止 • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-升级检查 • dms-replication-task-target db-记录 • dms-replication-task-source db-记录 • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-已启用 • 53 号公路-query-logging-enabled • rds-aurora-mysql-audit-启用日志功能 • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled • wafv2-rulegroup-logging-enabled	2023 年 9 月 21 日

	• msk-in-cluster-node-requi-tls	
Amazon Config 支持新的一致性包	在此版本中， Amazon Config 更新了以下一致性包： • Amazon S3 操作最佳实践 • 的操作最佳实践 EC2	2023 年 9 月 8 日
安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略现在会移除 Amazon Systems Manager （Systems Manager ）的权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2023 年 9 月 6 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的 Amazon P CodeGuru rofiler、、 AWS Elemental MediaConnect Amazon Transfer Family、Prom Amazon Batch etheus 的亚马逊托管服务、、和资源类型的配置更改。 Amazon Cloud Map Amazon Route 53 Resolver 有关更多信息，请参阅支持的资源类型。	2023 年 9 月 6 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • athena-workgroup-encrypted-at-休息 • neptune-cluster-iam-database-认证 • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-启用导出 • neptune-cluster-deletion-protection-已启用 • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-检查 • neptune-cluster-encrypted • neptune-cluster-snapshot-public-禁止 • docdb-cluster-backup-retention-检查 • docdb-cluster-encrypted • rds-cluster-encrypted-at-休息	2023 年 8 月 10 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对全新、亚马逊、亚马逊 Athena Amazon Amplify、亚马逊弹性计算云（亚马逊）AppIntegrations Amazon App Mesh、Amazon Evicently、Amazon Forecast、、、、、A CloudWatch mazon Man Amazon IoT Greengrass Version 2 aged Streaming Kafka（ EC2亚马逊 MSK）AWS Elemental MediaConvert AWS Elemental MediaTailor、Amazon Personalize、Amazon Pinpoint 和资源类型的配置更改。 Amazon Ground Station Amazon Resilience Hub 有关更多信息，请参阅支持的资源类型。	2023 年 8 月 3 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在授予亚马逊托管工作流程的额外权限，适用于亚马逊 WorkSpaces 应用程序 Amazon App Mesh、、亚马逊、、、Amazon Connect CloudFront Amazon CodeArtifact Amazon CodeBuild 、 Amazon Identity and Access Management （ IAM ） Amazon Glue、Amazon GuardDuty Inspector、、、、Amazon IoT、Amazon Macie Amazon IoT TwinMaker Amazon IoT Wireless、、、、、、、Amazon Route 53、亚马逊简单存储服务（Amazon S3） AWS Elemental MediaConnect Amazon Network Manager Amazon Organizations Amazon 资源探索器、亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 和亚马逊 Amazon CloudFormation EC2 Systems Manager (SSM)。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2023 年 7 月 28 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新的 Amazon Kinesis、亚马逊弹性计算云（亚马逊 EC2）、亚马逊 Pinpoint、亚马逊简单存储服务（亚马逊 S3）、亚马逊虚拟私有云（亚马逊 VPC）、亚马逊 Kendra、Amazon C Amazon CloudFormation onnect Amazon AppConfig 、、、和 () 资源类型的配置更改。 Amazon App Mesh Amazon App Runner Amazon Database Migration Service A mazon DMS有关更多信息，请参阅支持的资源类型。	2023 年 7 月 10 日
组织合规包的服务限制有所增加	在此版本中， Amazon Config 支持所有合 Amazon Config 规包中每个账户的每个区域 350 条规则，每个组织支持 350 Amazon Config 条组织规则。有关更多信息，请参阅服务限制。	2023 年 6 月 13 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊托管工作流程、Amazon Connect、Prometheus 的亚马逊托管服务 Amazon Amplify、Amazon Athena、、、、、Amazon App Mesh、、、、Amazon DynamoDB、亚马逊弹性计算云（亚马逊）、Amazon Evicently、Amazon Forecast、、、（I Amazon Batch AM）Amazon CloudFormation Amazon CloudTrail Amazon CodeArtifact、Amazon DynamoDB CodeGuru Amazon Directory Service、亚马逊弹性计算云（亚马逊）、Amazon Evicently、Amazon Forecast、、、（ EC2 Amazon Identity and Access Managemen t IAM）CloudWatch 、适用于 Apache 的亚马逊托管流媒体授予额外权限 Kafka Streaming Kafka（亚马逊 MSK）、亚马逊 Lightsail、Amazon Logs、 Amazon Organizations Amazon IoT Greengrass Amazon Ground Station CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor、亚马逊 Pinpoint、亚马逊虚拟私有	2023 年 6 月 13 日

云（亚马逊 VPC）、Amazon Personalize、Amazon Quick Suite、 Amazon Migration Hub Refactor Spaces亚马逊简单存储服务（亚马逊 S3）、亚马逊 AI 和 SageMaker Amazon Transfer Family有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。

Amazon Config 按资源类型记录排除项	在此版本中， Amazon Config 您可以将特定类型的 Amazon 资源排除在库存跟踪和合规性监控之外，同时仍可以跟踪中当前可用的所有其他受支持的资源类型 Amazon Config，包括将来将要添加的资源类型。您可以使用此功能将注意力集中在受合规性和监管标准约束的关键资源上。 配置记录器和录制组的 API 更新向后兼容，这意味着它们可以与以前版本的 PutConfigurationRecorderAPI 一起使用。您可以继续以与以前完全相同的方式管理记录哪些资源类型，而无需使用更新的或新的资源类型 APIs。 将添加以下数据类型： • RecordingStrategy • ExclusionByResourceTypes 将更新以下数据类型： • PutConfigurationRecorder • ConfigurationRecorder • RecordingGroup 将更新开发人员指南中的以下页面： • 选择所记录的资源	2023 年 6 月 9 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新的亚马逊弹性容器服务 (Amazon ECS)、亚马逊密钥空间（适用于 Apache Cassandra）（亚马逊密钥空间）、、、、、、、、亚马逊弹性计算云（亚马逊）、Amazon Evicently、Amazon Forecast Amazon Signer、(IAM Amazon Amplify) Amazon App Mesh、Amazon Pinpoint Amazon App Runner WorkSpaces 、Amazon Amazon CodeArtifact Evisently 、Amazon Forecast、EC2（IAM）、 CloudWatch Amazon Pinpoint、Amazon Pinpoint、Amazon Amazon Identity and Access Management AI、、Amazon Data F SageMaker irehose 资源类型。 Amazon Transfer Family有关更多信息，请参阅支持的资源类型。	2023 年 6 月 5 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • 云前线-3-origin-access-control-enabled • custom-schema-registry-policy-已附上 • ec2-client-vpn-not-authorize-全部 • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-已启用升级 • mq-cloudwatch-audit-logging-已启用 • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-启用日志功能	2023 年 5 月 10 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的、亚马逊弹性计算云（亚马逊 EC2）、 Amazon IoT 无线 Amazon Route 53 Resolver、、、、亚马逊、Redshift、Amazon Pinpoint Amazon Network Manager Amazon Device Farm Amazon Ground Station、、 AppFlow、、Im Amazon AppConfig age EC2 Builder、Amazon、Amazon Amazon IoT、、Amazon R SageMaker untime CloudWatch Amazon Panorama、Amazon ECR 和资源类型的配置更改。 Amazon Audit Manager 有关更多信息，请参阅支持的资源类型。	2023 年 5 月 5 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对的配置更改`AWS::NetworkFirewall::TLSInspectionConfiguration` 。有关更多信息，请参阅支持的资源类型。	2023 年 5 月 1 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在授予亚马逊托管工作流程的额外权限，包括、、、亚马逊 Amazon Amplify、、Amazon App Mesh亚马逊 Elastic Compute Cloud CloudFront Amazon CodeArtifact、Amazon Kendra、Amazon Macie、Amazon Route 53、Amazon A Amazon Transfer Family I、Amazon Pinpoint、、 SageMaker Resilience Hub、亚马逊 Amazon Migration Hub Amazon 、Di Amazon rectory Service 和。 Amazon App Runner CloudWatch Amazon WAF有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2023 年 4 月 13 日

Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • elasticache-auto-minor-version-升级检查 • elasticache-repl-grp-auto-启用故障转移 • elasticache-repl-grp-encrypted-在休息时 • elasticache-repl-grp-encrypted在途中 • elasticache-repl-grp-redis-已启用 auth • elasticache-subnet-group-check • 云前线-3-origin-non-existent-bucket	2023 年 4 月 10 日
组织合规包的服务限制有所增加	在此版本中，所有组织一致性包 Amazon Config 支持每个账户 350 Amazon Config 条规则。有关更多信息，请参阅服务限制。	2023 年 4 月 3 日

Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-休息	2023 年 4 月 3 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新亚马逊 WorkSpaces 应用程序、A Amazon uto Scaling、Amazon Connect 亚马逊弹性计算云、亚马逊、、Kinesis 视频流 EventBridge HealthLake、Lookout for Vision Amazon IoT TwinMaker、网络管理器、亚马逊 Pinpoint、亚马逊应用程序恢复控制器 (ARC) 和资源类型的配置更改。 Amazon RoboMaker 有关更多信息，请参阅支持的资源类型。	2023 年 4 月 3 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊、亚马逊 WorkSpaces 应用程序、、亚马逊、亚马逊 AppFlow、、、、 Amazon App Runner、亚马逊弹性计算云（亚马逊） Amazon CloudFormation CloudFront、Amazon CloudWatch Evidently CloudWatch Amazon CodeArtifact Amazon CodeCommit Amazon Device Farm、Amazon Forecast、 Amazon Identity and Access Management （IAM EC2）、、Amazon MemoryDB Amazon Ground Station、Amazon Pinpoint Amazon IoT、、、、亚马逊关系数据库 Amazon Panorama 服务（亚马逊 RDS） Amazon Network Manager、Amazon Redshift 和亚马逊 AI。SageMaker 有关更多信息，请参阅适用于 Amazon Config的 Amazon 托管策略。	2023 年 3 月 30 日
安全 IAM 更新	AWSConfigServiceRolePolicy 策略和 AWS_ConfigRole 策略现在为 Amazon Audit Manager授予更多权限。有关更多信息，请参阅适用于 Amazon Config的 Amazon 托管策略。	2023 年 3 月 3 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的、亚马逊、 AWS Elemental MediaPackage、（亚马逊简单存储服务 (Amazon S3) EventBridge Amazon IoT、亚马逊弹性计算云（亚马逊）、亚马逊 Lookout for Metrics、 EC2 Amazon Lex、、、、Amazon Amazon Budgets Amazon Route 53 Resolver Reviewer 和资源类型的配置更改。 Amazon Device Farm CodeGuru Amazon RoboMaker 有关更多信息，请参阅支持的资源类型。	2023 年 3 月 2 日
安全 IAM 更新	Amazon Config 现在可以跟踪`AWSConfigMultiAccountSetupPolicy` 策略的更改。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2023 年 2 月 27 日
Amazon Config 按地区可用性划分的资源覆盖率	在此版本中， Amazon Config 为每种支持的资源类型提供了区域信息。有关哪些区域支持哪些资源类型的信息，请参阅按区域可用性列出的资源覆盖范围。	2023 年 2 月 20 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的亚马逊互动视频服务 (Amazon IVS)、亚马逊简单存储服务 (Amazon Amazon Glue S3)、亚马逊 Elastic Kubernetes 服务 (Amazon EKS)、亚马逊 Amazon IoT关系数据库服务 (Amazon RDS) 和 Apache Flink 托管服务资源的配置更改类型。有关更多信息，请参阅支持的资源类型。	2023 年 2 月 7 日
安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为Apache Airflow、Amazon Applications、Amazon Reviewer Amazon IoT、Ama WorkSpaces zon Kinesis Video Streams Amazon HealthLake、 CodeGuru 亚马逊应用程序恢复控制器 (ARC)、亚马逊弹性计算云 (亚马逊) Amazon Device Farm、Amazon Pinpoin Amazon Identity and Access Management t、(IAM EC2)、亚马逊和亚马逊日志的亚马逊托管工作流程授予额外权限。 GuardDuty CloudWatch 有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2023 年 2 月 1 日

安全 IAM 更新	作为安全最佳实践，`ConfigConformsServiceRolePolicy` 策略现在取消了对 `config:DescribeConfigRules` 的广泛资源级别权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2023 年 1 月 12 日
安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为亚马逊托管服务 Prometheus Amazon Audit Manager、 Amazon Device Farm、、、、、、、、、Amazon Elightsail、、、 Amazon Directory Service、Amazon Quick Suite、、 Amazon Glue、EC2 Amazon IoT亚马逊应用程序恢复控制器 (ARC Amazon DMS) AWS Elemental MediaPackage、 Amazon Network Manager亚马逊简单存储服务 (Amazon S3) Simple Service 和 Amazon Timestream 授予额外权限。 Amazon Database Migration Service Amazon Resource Access Manager有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2023 年 1 月 10 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新亚马逊 MQ、、、 Amazon Cloud9亚马逊 EventBridge 架构、 Amazon AppConfig Amazon Fraud Detector、、、、Amazon Amazon IoT Analytics Lightsail、(AWS Elemental MediaPackage) MediaPackage、亚马逊应用程序恢复控制器 (ARC) 和资源类型的配置更改。 Amazon IoT Amazon Resilience Hub Amazon Transfer Family 有关更多信息，请参阅支持的资源类型。	2023 年 1 月 5 日
Amazon Config 规则资源覆盖范围	在此版本中， Amazon Config 显示更多 Amazon Config 托管规则的资源类型覆盖范围。	2022 年 12 月 21 日
Amazon Config 规则可发现性	在此版本中， Amazon Config 支持 “按评估模式划分的 Amazon Config 托管规则列表”、“按触发器类型划分的 Amazon Config 托管规则列表” 和 “按区域可用性划分的 Amazon Config 托管规则列表” 的页面。	2022 年 12 月 21 日

Amazon Config 支持新的一致性包	在此版本中， Amazon Config 更新了以下一致性包： • K-ISMS 操作最佳实践 • NIST 800 171 操作最佳实践 • PCI DSS 3.2.1 操作最佳实践 • Esquema Nacional de Seguridad（ ENS ）High 操作最佳实践 • Esquema Nacional de Seguridad（ ENS ）Medium 操作最佳实践 • Esquema Nacional de Seguridad（ ENS ）Low 操作最佳实践 • NZISM 操作最佳实践 • NIST 800-53 rev 5 操作最佳实践	2022 年 12 月 19 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • api-gwv2-access-logs-enabled • api-gwv2-authorization-type-configured • cloudfront-security-policy-check • ec2-launch-template-public-ip-已禁用 • elastic-beanstalk-logs-to-云观察 • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-访问检查 • security-account-information-provided • storagegateway-resources-protected-by-备份计划 • wafv2-rulegroup-not-empty • wafv2-webacl-not-empty	2022 年 12 月 9 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的 Amazon CloudWatch RUM、亚马逊、亚马逊 EventBridge GuardDuty、亚马逊简单电子邮件服务 (Amazon SES) Amazon Backup、 Amazon DataSync、 Amazon Fault Injection Service 和Amazon FIS() 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 12 月 9 日

Amazon Config 主动合规	在此版本中，Amazon Config 支持在资源调配之前主动检查 Amazon Config 规则的合规性。这允许您在创建或更新资源之前评估资源的配置设置。用于跟踪 Amazon Config 对资源所做的配置更改（无论是预配置前还是置备后），并检查您的资源是否与所需的配置相匹配。 将添加以下数据类型： • GetResourceEvaluationSummary • StartResourceEvaluation • ListResourceEvaluations 将更新以下数据类型： • DescribeConfigRulesFilters • GetComplianceDetailsByResource • EvaluationResultQualifier • EvaluationModeConfiguration 将更新开发人员指南中的以下页面： • Amazon Config 规则的组成部分 • Amazon Config 规则的评估模式和触发器类型 • Amazon Config 托管规则	2022 年 11 月 28 日

	• Amazon Config 自定义规则 • 管理您的 Amazon Config 规则	
将偏差检测作为配置记录器的 Amazon Config 配置项目 (CI)	在此版本中， Amazon Config 跟踪对配置记录器的所有更改，以指示配置记录器的状态是否与其先前的状态不同或有所偏差；例如，是否有已启用 Amazon Config 跟踪的资源类型的更新，是否已停止或启动配置记录器，或者是否已删除或卸载配置记录器。`AWS::Config::ConfigurationRecorder` 资源类型是系统资源类型，默认情况下 Amazon Config ，所有支持的区域都启用了该资源类型的记录。`AWS::Config::ConfigurationRecorder` 资源类型的记录不收取额外费用。有关更多信息，请参阅配置记录器的偏差检测。	2022 年 11 月 18 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新、、EC2 Image Builder Amazon IoT Events、、、 Amazon Cloud Map Amazon DataSync Amazon Glue、亚马逊应用程序恢复控制器 (ARC) 和亚马逊弹性容器注册表 (Amazon ECR) Elastic Registry 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 11 月 8 日

安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略和 `AWS_ConfigRole` 策略现在为 Amazon CloudFormation授予更多权限。有关更多信息，请参阅适用于 Amazon Config 的Amazon 托管策略。	2022 年 11 月 7 日
Amazon Config 支持新的一致性包	在此版本中， Amazon Config 支持以下一致性包： • 刑事司法信息服务（CJIS）操作最佳实践 • Amazon A SageMaker I 安全最佳实践 • Amazon Elastic Container Registry 安全最佳实践 将更新以下合规包： • MAS TRMG 操作最佳实践 • NCSC 网络评估框架操作最佳实践 • NCSC 云安全原则操作最佳实践	2022 年 10 月 27 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊管理的 Apache Airflow 工作流程 Amazon Certificate Manager、、、Amazon Keyspaces Amazon Amplify、 Amazon AppConfig亚马逊、Amazon Connect Amazon Glue DataBrew、亚马逊弹性计算云（亚马逊） CloudWatch、亚马逊弹性 Kubernetes 服务（亚马逊 EKS）、亚马逊、 EC2亚马逊 Fraud Detector、亚马逊、亚马逊服务器、亚马逊定位服务授予额外权限 Service EventBridge、、 Amazon Fault Injection Service Amazon Lex FSx、Amazon Lightsail、A GameLift mazon Pinpoint Amazon IoT、、、、Amazon Quick Amazon OpsWorks Amazon Panorama Amazon Resource Access Manager 套件、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Amazon RoboMaker Rekognition、、、Amazon Route 53 Amazon Resource Groups、亚马逊简单存储服务 Amazon Cloud Map(Amazon S3)、Amazon Simple Storage Service 和。 Amazon Security Token Service有关更多信息，	2022 年 10 月 19 日

	请参阅适用于 Amazon Config 的Amazon 托管策略。	
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的亚马逊弹性计算云 (Amazon EC2)、亚马逊简单电子邮件服务 (Amazon SES) Amazon AppConfig Amazon Cloud Map、 Amazon DataSync 和资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 10 月 6 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新的 Amazon GuardDuty、Amazon A SageMaker I、 Amazon AppSync Amazon Cloud Map、和 Amazon DataSync 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 10 月 4 日
Amazon Config 支持新的一致性包	在本版本中， Amazon Config 更新了 SWIFT CSP 一致性包的运营最佳实践。	2022 年 10 月 4 日

Amazon Config 支持新的一致性包	在此版本中， Amazon Config 支持以下一致性包： • CMMC 2.0 Level 1 操作最佳实践 • CMMC 2.0 Level 2 操作最佳实践 将更新以下合规包： • Amazon API Gateway 操作最佳实践 • Well-Architecte Amazon d 框架可靠性支柱的运营最佳实践 • Well-Architecte Amazon d Framework 安全支柱的运营最佳实践 • CMMC Level 1 操作最佳实践 • CMMC Level 2 操作最佳实践 • CMMC Level 3 操作最佳实践 • CMMC Level 4 操作最佳实践 • CMMC Level 5 操作最佳实践 • FFIEC 操作最佳实践 • FedRAMP(Low) 操作最佳实践 • MAS 第 655 号通知操作最佳实践 • NBC TRMG 操作最佳实践	2022 年 9 月 30 日

	• NIST 800 172 操作最佳实践	
安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略和 `AWS_ConfigRole` 策略现在为 Amazon Glue授予更多权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2022 年 9 月 14 日
Amazon Config 支持新的一致性包	在本版本中， Amazon Config 支持 SWIFT CSP 一致性包的运营最佳实践。	2022 年 9 月 9 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊 AppFlow、亚马逊、亚马逊 R CloudWatchUM、Amazon S CloudWatch ynthetics CloudWatch、Amazon Connect 客户档案、Amazon Connect 语音识别码、Amazon DevOps Guru、亚马逊弹性计算云（亚马逊）、Amazon Aut EC2 o Scaling EC2、亚马逊 EMR、亚马逊、亚马逊 Schemas、Amazon Fraud Detector、EventBridge亚马逊 GameLift 服务器、 EventBridge 亚马逊互动视频服务授予额外权限（IVS) Interactive Service、适用于 Apache Flink 的亚马逊托管服务、Image Builder Amazon FinSpace EC2 、亚马逊 Lex、亚马逊 Lightsail 、亚马逊定位服务、亚马逊 Lookout for Equite、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble Pinpoint、StudioAmazon Amazon Quick Suite、亚马逊应用程序恢复 Amazon Route 53 Resolver控制器 (ARC)、亚马逊简单存储服务（亚马逊 S3）、亚马逊 SimpleDB、亚马逊简单电子邮件服务 (亚马逊 SES)、亚马逊	2022 年 9 月 7 日

Timestream、、、

Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包： • Amazon 最佳运营实践 CloudWatch • 德国云计算合规性控制目录（C5）操作最佳实践 • IRS 1075 操作最佳实践 将更新以下合规包： • Amazon Control Tower Detective Guardrails 一致性包 • CISA Cyber Essentials 操作最佳实践 • ENISA 运营最佳实践网络安全指南 SMEs • FDA 联邦法规第 21 篇第 11 部分操作最佳实践 • FedRAMP(Moderate）操作最佳实践 • HIPAA 安全操作最佳实践 • NIST 隐私框架 v1.0 操作最佳实践 • NYDFS 23 操作最佳实践 • 印度储备银行网络安全框架的最佳运营实践 UCBs • RBI MD-ITF 操作最佳实践	2022 年 8 月 31 日

入门 Amazon Config 和自定义一致性包更新	在此版本中， Amazon Config 更新了 “控制台入门” Amazon Config和 “使用控制台 Amazon Config 进行设置” 页面，引入了 “一键设置” 和 “手动设置” 页面。 Amazon Config 还更新了自定义一致性包页面，其中包含有关如何从头开始创建一致性包 YAML 文件的演练。	2022 年 8 月 25 日
Amazon Systems Manager 文档（SSM 文档）与一致性包集成	在此版本中，您可以使用 SSM 文档创建合规包模板。有关 SSM 文档的更多信息，请参阅《 Amazon Systems Manager 用户指南》中的 Amazon Systems Manager 文档。 将更新以下数据类型： • PutConformancePack • ConformancePackDetail • 模板SSMDocument详情 将更新开发人员指南中的以下页面： • 使用控制台部署一致性包 Amazon Config • 使用 Amazon 命令行界面部署一致性包	2022 年 8 月 24 日

安全 IAM 更新	现在，该AWSConfig ServiceRolePolicy 策略和AWS_ConfigRole 策略授予亚马逊简单电子邮件服务 (Amazon SES) Amazon DataSync、 Amazon Cloud Map和的额外权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2022 年 8 月 22 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的 Amazon Athena、Amazon Detective、Amazon AI、Amazon Rout SageMaker e Amazon Database Migration Service 53、()Amazon DMS、() 和亚马逊简单电子邮件服务 (Amazon SES Amazon Glue) Amazon Key Managemen t Service Service (Amazon SES) 资源类型的配置更改。Amazon KMS有关更多信息，请参阅支持的资源类型。	2022 年 8 月 16 日

Amazon Config 支持新的一致性包	在此版本中， Amazon Config 更新了以下一致性包： • NIST 1800 25 操作最佳实践 • NIST 800 181 操作最佳实践 • ABS CCIG 2.0 标准工作负载操作最佳实践 • ABS CCIG 2.0 重要工作负载操作最佳实践 • ACSC Essential 8 操作最佳实践 • ACSC ISM 操作最佳实践 • APRA CPG 234 操作最佳实践 • CIS Amazon 基金会运营最佳实践基准 v1.4 第 1 级 • CIS Amazon 基金会运营最佳实践基准 v1.4 第 2 级 • BNM RMi T 的最佳运营实践 • NIST CSF 操作最佳实践	2022 年 8 月 1 日

合规包的合规性分数	在此版本中，Amazon Config 引入了一致性包的合规性分数，它使您能够从高层次了解合规包的合规性状态。您可以使用此分数来识别、调查和了解合规包中的合规性级别。合规性分数是合规包中的合规规则资源组合数量与合规包中可能的规则资源组合总数的百分比。 将更新以下数据类型： • ListConformancePackComplianceScores • ConformancePackComplianceScore 将更新开发人员指南中的以下页面： • 查看 Amazon Config 控制面板 • 在“合规包”控制面板中查看合规性数据 • 管理合规包（API）	2022 年 7 月 26 日
安全 IAM 更新	该`ConfigConformsServiceRolePolicy` 政策现在授予向亚马逊发布指标数据点的权限 CloudWatch。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2022 年 7 月 25 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊弹性容器服务 (Amazon ECS)、亚马逊、亚马逊、亚马逊、适用于 Apache Flink 的亚马逊托管服务 EventBridge、亚马逊定位服务 FSx、适用于 Apache Kafka 的亚马逊托管流媒体、亚马逊 Quick Suite、亚马逊 Rekognition、亚马逊简单存储服务 (亚马逊 S3) 授予额外权限)、Ama Amazon RoboMaker zon Semple Email Service (Amazon SES)、、、、、、、、、、（IAM 身份中心）Amazon Amplify、 ElastiCache Amazon AppConfig Amazon AppSync Amazon Billing Conductor Amazon DataSync Amazon Firewall Manager Amazon Glue Amazon IAM Identity Center EC2 Image Builder 和 Elastic Load Balancing。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2022 年 7 月 15 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新的亚马逊弹性计算云 (Amazon EC2) 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 7 月 8 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新 Amazon Global Accelerator 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 7 月 5 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • autoscaling-launch-template • ecs-task-definition-log-配置 • ecs-awsvpc-networking-enabled	2022 年 7 月 1 日

Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包： • 加拿大网络安全中心（CCCS）Medium Cloud Control Profile 操作最佳实践 • 《格雷姆-里奇-布里利法案》(GLBA）操作最佳实践 • GxP 欧盟附件 11 操作最佳实践 • Amazon Elastic Kubernetes Service（Amazon EKS）安全最佳实践 • Amazon Relational Database Service（Amazon RDS）安全最佳实践 • 的安全最佳实践 Amazon Lambda 将更新以下合规包： • 人工智能和机器学习操作最佳实践 • Amazon DynamoDB 操作最佳实践 • CIS 关键安全控制操作最佳实践 v8 IG1 • CIS 关键安全控制操作最佳实践 v8 IG2 • CIS 关键安全控制操作最佳实践 v8 IG3 • HIPAA 安全操作最佳实践 • NIST 800-53 rev 5 操作最佳实践	2022 年 6 月 30 日

	• NIST CSF 操作最佳实践	
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新 Amazon A SageMaker I 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 6 月 29 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录适用于Apache Kafka（亚马逊 MSK）、亚马逊 Route 53、亚马逊、（IAM Access Amazon Database Migration Service Analyzer） WorkSpaces、Amazon Batch(Amazon DMS) 和 Elastic Load Balancing 的新资源类型的配置更改。Amazon Identity and Access Management Access Analyzer Amazon Step Functions有关更多信息，请参阅支持的资源类型。	2022 年 6 月 14 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • aurora-last-backup-recovery-已创建积分 • dynamodb-last-backup-recovery-已创建积分 • ebs-last-backup-recovery-已创建积分 • ec2-已last-backup-recovery-point创建 • efs-last-backup-recovery-已创建积分 • fsx-last-backup-recovery-已创建积分 • rds-last-backup-recovery-已创建积分 • s3-已last-backup-recovery-point创建 • storagegateway-last-backup-recovery-已创建积分 • virtualmachine-last-backup-recovery-已创建积分	2022 年 6 月 13 日

Amazon Config 与集成 Amazon Security Hub CSPM	在此版本中，您可以在中查看 Amazon Config 托管规则和自定义规则评估的结果 Amazon Security Hub CSPM。Security Hub CSPM 将规则评估转化为调查结果，从而提供有关受影响资源的更多信息，例如亚马逊资源名称 (ARN) 和创建日期。这些调查发现可与其他 Security Hub CSPM 调查发现一起查看，提供您的安全态势的全面概述。有关更多信息，请参阅向 Security Hub CSPM 发送规则评估	2022 年 6 月 7 日
安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊 Athena、Amazon Detective、亚马逊、亚马 GuardDuty逊 Macie、亚马逊简单电子邮件服务 (Amazon Amazon Glue S Amazon Resource Access Manager ES)、、() 和授予额外权限。Amazon RAM Amazon IAM Identity Center有关更多信息，请参阅适用于 Amazon Config 的Amazon 托管策略。	2022 年 5 月 31 日

Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包： • Amazon Elastic Container Service（Amazon ECS）安全最佳实践 • Amazon Elastic File System（Amazon EFS）安全最佳实践 • Amazon 安全最佳实践 CloudFront • 的安全最佳实践 Amazon Auto Scaling • 的安全最佳实践 Amazon Network Firewall • 的安全最佳实践 Amazon Secrets Manager	2022 年 5 月 31 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新 Amazon A SageMaker I 和 Amazon Step Functions 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 5 月 26 日
Amazon Config 支持新的一致性包	在此版本中，Amazon Config 更新了 NERC CIP BCSI 一致性包的操作最佳实践。	2022 年 5 月 20 日

Amazon Config 规则的组成部分	在此版本中，Amazon Config 引入了 “Amazon Config 规则组件” 页面。该页面讨论了规则定义的结构、规则元数据以及如何使用规则开发套件 (RDK) 和 Amazon Config 规则开发套件库 (RDKlib) 使用 Python 编写 Amazon Config 规则的最佳实践。	2022 年 5 月 9 日
组织合规包的服务限制有所增加	在此版本中，Amazon Config 支持所有组织一致性包中每个账户 180 Amazon Config 条规则。有关更多信息，请参阅服务限制。	2022 年 5 月 6 日
Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包： • Amazon OpenSearch 服务安全最佳实践 • Amazon Redshift 安全最佳实践 • 的安全最佳实践 Amazon CloudTrail • 的安全最佳实践 Amazon CodeBuild • 的安全最佳实践 Amazon WAF	2022 年 4 月 29 日
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持 s 3 resources-protected-by-backup-计划托管规则。	2022 年 4 月 11 日

安全 IAM 更新	现在，该AWSConfig ServiceRolePolicy AWS_ConfigRole 策略和策略授予其他权限，以获取有关所有或指定 Amazon CloudTrail 事件数据存储 (EDS) 的信息，获取有关所有或指定 Amazon CloudFormation 资源的信息，获取 DynamoDB Accelerator (DAX) 参数组或子网组的列表，获取 Amazon Database Migration Service 有关当前正在访问的区域中您的账户的Amazon DMS() 复制任务的信息，以及获取指定类型的所有策略的列表。 Amazon Organizations 有关更多信息，请参阅适用于 Amazon Config 的Amazon 托管策略。	2022 年 4 月 7 日

Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-极限 • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-版本 • netfw-policy-default-action-碎片数据包 • netfw-policy-default-action-满包 • netfw-policy-rule-group-关联 • redshift-audit-logging-enabled • s3-lifecycle-policy-check • waf-regional-rule-not-空 • waf-regional-rulegroup-not-空 • waf-regional-webacl-not-空 • vpc-peering-dns-resolution-检查	2022 年 4 月 22 日

Amazon Config 自定义策略规则	在此版本中，Amazon Config 允许您使用 Amazon CloudFormation Guard（guard）创建 Amazon Config 自定义策略规则。Guard 是一种允许您编写由其强制执行的策略的 policy-as-code语言，Amazon Config 而无需创建 Lambda 函数来管理您的自定义规则。使用 Guard 策略编写的规则可以从 Amazon Config 控制台创建，也可以使用 Amazon Config 规则创建 APIs。 将更新开发人员指南中的以下页面： • Amazon Config 自定义规则 • 使用 Guard 创建 Amazon Config 自定义规则 将更新以下数据类型： • 源 • CustomPolicyDetails • ConfigRuleEvaluationStatus • GetCustomRulePolicy • GetOrganizationCustomRulePolicy • OrganizationCustomPolicyRuleMetadata	2022 年 4 月 22 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新 Amazon EMR SecurityConfiguration 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 3 月 31 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持 virtualmachine-resources-protected-by-backup-plan 托管规则。	2022 年 3 月 29 日
Amazon Config 与 Amazon CloudWatch 指标集成	在此版本中， Amazon Config 现在支持在 Amazon Config 控制面板页面 CloudWatch 中 Amazon Config 使用亚马逊跟踪您的使用情况和成功指标。 CloudWatch metrics 是一项监控服务，可提供有关系统性能的数据，包括根据有关 Amazon 资源的指标进行搜索、绘制图表和生成警报的能力。在 Amazon Config 控制面板中，您可以看到哪些流量推动了您的 Amazon Config 使用量，以及工作流程中出现的故障的关键指标。 将更新以下页面： • 查看 Amazon Config 控制面板	2022 年 3 月 29 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新 Amazon Det GuardDuty ector 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 3 月 24 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • clb-multiple-az • cloudfront-no-deprecated-ssl-协议 • cloudfront-traffic-to-origin-已加密 • cloudwatch-alarm-action-enabled-检查 • ec2-no-amazon-key-pair • ec2-paravirtual-instance-check • ec2-token-hop-limit-check • ec2-transit-gateway-auto-vpc-已禁用附件 • ecr-private-lifecycle-policy-已配置 • efs-access-point-enforce-根目录 • efs-access-point-enforce-用户身份 • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-检查 • s3-event-notifications-enabled • sns-topic-message-delivery-启用通知 • waf-global-rulegroup-not-空 • waf-global-rule-not-空	2022 年 3 月 23 日

Amazon Config 支持新的一致性包	在此版本中， Amazon Config 更新了以下一致性包： • CIS 关键安全控制操作最佳实践 v8 IG1 • CIS 关键安全控制操作最佳实践 v8 IG2 • CIS 关键安全控制操作最佳实践 v8 IG3 • Well-Architecte Amazon d Framework 安全支柱的运营最佳实践 • Esquema Nacional de Seguridad（ ENS ）Low 操作最佳实践 • Esquema Nacional de Seguridad（ ENS ）Medium 操作最佳实践 • Esquema Nacional de Seguridad（ ENS ）High 操作最佳实践 • MAS 第 655 号通知操作最佳实践 • NIST 1800-25 操作最佳实践	2022 年 3 月 16 日
安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略和 `AWS_ConfigRole` 策略现在为 Amazon CloudFormation授予更多权限。有关更多信息，请参阅适用于 Amazon Config 的Amazon 托管策略。	2022 年 3 月 14 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 更新了以下托管规则： • aurora-resources-protected-by-备份计划 • dynamodb-resources-protected-by-备份计划 • ebs-resources-protected-by-备份计划 • ec2 resources-protected-by-backup-计划 • efs-resources-protected-by-备份计划 • fsx-resources-protected-by-备份计划 • rds-resources-protected-by-备份计划	2022 年 3 月 10 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新 Amazon Elastic Container Registry 公共资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 3 月 4 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新的 Amazon 弹性计算云资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 2 月 28 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • codedeploy-auto-rollback-monitor-已启用 • codedeploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-禁用	2022 年 2 月 25 日
Amazon Config 更新中的日志和监控	在此版本中，Amazon Config 更新了 “Amazon Config 使用亚马逊 EventBridge 事件监控” 页面，以取代对亚马逊 CloudWatch 事件的引用。亚马逊 EventBridge 是管理您的活动的首选方式。 CloudWatch 事件和 EventBridge 是相同的底层服务和 API，但 EventBridge 提供了更多功能。您在 CloudWatch 或中所做的更改 EventBridge 将显示在每个主机中。有关更多信息，请参阅 Amazon EventBridge。	2022 年 2 月 24 日
Amazon 适用于 SDK 的页面 Amazon Config	在此版本中，Amazon Config 引入了 “Amazon Config 使用 S Amazon DK” 页面。 Amazon 软件开发套件 (SDKs) 可用于许多流行的编程语言。每个软件开发工具包都提供 API、代码示例和文档，使开发人员能够更轻松地以其首选语言构建应用程序。	2022 年 2 月 24 日

安全 IAM 角色信任策略更新	在此版本中， Amazon Config 更新了 IAM 信任策略声明，以在信任策略中加入安全保护，从而限制对 Amazon Security Token Service (Amazon STS) 操作`sourceARN` and/or `sourceAccountId` 的访问。这有助于确保 IAM 角色策略仅代表预期用户和场景访问您的资源。 将更新以下页面： • 将 IAM 信任策略添加到您的角色	2022 年 2 月 18 日

对全局资源类型记录的更改	Amazon Config 现在更改了录制中新的全局资源类型的 Amazon Config 录制方式。全局资源类型是指不需要您在创建时指定区域的 Amazon 资源。在此更改之前，您可以启用 Amazon Config中所有支持区域中全局资源类型的记录。进行此更改后，新加入录制的全局资源类型只能在服务主区域 Amazon Config 录制商业分区，（美国西部）只能在分区的 Amazon GovCloud （美国西部）中录制。 Amazon GovCloud (US) 现在，您只能在其所在地区和 Amazon GovCloud （美国西部）查看这些新的全球资源类型的配置项目。有关 2022 年 2 月之后载入的全局资源类型的主区域列表，请参阅记录所有受支持的资源类型页面上的表格。	2022 年 2 月 18 日

安全 IAM 更新	现在，该AWSConfig ServiceRolePolicy 策略和AWS_ConfigRole 策略授予以下权限：获取有关 Elastic Beanstalk 环境的详细信息以及对指定 Elastic Beanstalk 配置集的设置的描述，获取我们的 Elasticsearch 版本地图，描述数据库 OpenSearch 的可用的 Amazon RDS 选项组，以及获取有关部署配置的信息。 CodeDeploy 现在，该策略还授予以下权限：检索附加到的指定备用联系人 Amazon Web Services 账户、检索有关 Amazon Organizations 策略的信息、检索 Amazon ECR 存储库策略、检索有关存档 Amazon Config 规则的信息、检索 Amazon ECS 任务定义系列列表、列出指定子 OU 或账户的根或上级组织单位 (OUs)，以及列出附加到指定目标根目录、组织单位或账户的策略。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2022 年 2 月 10 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-检查 • codebuild-project-logging-enabled • codebuild-project-s3 个日志加密 • ec2-security-group-attached-to-eni-peric • ecr-private-image-scanning-已启用 • ecr-private-tag-immutability-已启用 • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-硬限制 • ecs-task-definition-nonroot-用户 • ecs-task-definition-pid-模式检查 • eks-cluster-oldest-supported-版本 • eks-cluster-supported-version	2022 年 2 月 10 日

	• lambda-vpc-multi-az-检查 • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-不为空 • rds-cluster-default-admin-检查 • rds-db-security-group-不允许 • rds-instance-default-admin-检查 • redshift-default-admin-check • s3-bucket-acl-prohibited • s3-version-lifecycle-policy-check • waf-global-webacl-not-空	
安全 IAM 更新	现在，该AWSConfig ServiceRolePolicy 策略和AWS_ConfigRole 策略授予创建 Amazon CloudWatch 日志组和流以及向已创建的日志流写入日志的权限。有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2022 年 2 月 2 日

Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-容忍 • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-加密检查	2022 年 1 月 31 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录 Amazon CodeDeploy 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 1 月 5 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新 Amazon A SageMaker I 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 12 月 20 日
Amazon Config 支持新的一致性包	在此版本中， Amazon Config 支持以下一致性包： • ENISA 运营最佳实践网络安全指南 SMEs	2021 年 12 月 20 日

Amazon Config 支持新的一致性包	在此版本中， Amazon Config 支持以下一致性包： • NIST 800 172 操作最佳实践 • NIST 800 181 操作最佳实践 将更新以下合规包： • K-ISMS 操作最佳实践	2021 年 11 月 18 日
Amazon Config 支持新的一致性包	在此版本中， Amazon Config 支持以下一致性包： • Amazon API Gateway 操作最佳实践 • 的操作最佳实践 Amazon Backup • CISA Cyber Essentials 操作最佳实践 • 的操作最佳实践 DevOps • NIST 隐私框架 v1.0 操作最佳实践 将更新以下合规包： • FedRAMP(Low) 操作最佳实践 • FedRAMP(Moderate) 操作最佳实践	2021 年 10 月 29 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对新 Amazon S OpenSearch ervice 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 10 月 12 日

Amazon Config 支持新的一致性包	在此版本中，Amazon Config 更新了以下一致性包： • MAS TRMG 操作最佳实践	2021 年 10 月 12 日

Amazon Config 支持新的一致性包	在此版本中，Amazon Config 更新了以下一致性包： • ABS CCIG 2.0 重要工作负载操作最佳实践 • ABS CCIG 2.0 标准工作负载操作最佳实践 • ACSC Essential 8 操作最佳实践 • ACSC ISM 操作最佳实践 • BNM RMi T 的最佳运营实践 • CMMC Level 1 操作最佳实践 • CMMC Level 2 操作最佳实践 • CMMC Level 3 操作最佳实践 • CMMC Level 4 操作最佳实践 • CMMC Level 5 操作最佳实践 • 适用于 FDA 联邦法规第 21 篇第 11 部分的运营最佳实践 • 适用于 FFIEC 的运营最佳实践 • MAS 第 655 号通知操作最佳实践 • NBC TRMG 操作最佳实践 • NERC CIP 操作最佳实践 • NIST 800-53 rev 5 操作最佳实践	2021 年 9 月 30 日

安全 IAM 更新	现在，该AWS_ConfigRole 策略和AWSConfigServiceRolePolicy 政策授予获取有关亚马逊 OpenSearch 服务（OpenSearch 服务）的详细信息 domain/domains 以及获取特定亚马逊关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表的权限。该政策还授予获取有关 Amazon ElastiCache 快照的详细信息的权限。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2021 年 9 月 8 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录新的 Amazon 弹性计算云资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 9 月 7 日

Amazon Config 支持新的一致性包	在此版本中， Amazon Config 更新了以下一致性包： • APRA CPG 234 操作最佳实践 • CIS Amazon 基金会运营最佳实践基准 v1.4 第 1 级 • CIS Amazon 基金会运营最佳实践基准 v1.4 第 2 级 • NCSC 云安全原则操作最佳实践 • NCSC 网络评估框架操作最佳实践 • NIST 800 171 操作最佳实践 • NIST CSF 操作最佳实践 • 印度储备银行网络安全框架的最佳运营实践 UCBs • RBI MD-ITF 操作最佳实践 • NYDFS 23 操作最佳实践 • PCI DSS 3.2.1 操作最佳实践	2021 年 8 月 30 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • aurora-resources-protected-by-备份计划 • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-删除-禁用 • backup-recovery-point-minimum-保留检查 • dynamodb-resources-protected-by-备份计划 • ebs-resources-protected-by-备份计划 • ec2 resources-protected-by-backup-计划 • efs-resources-protected-by-备份计划 • fsx-resources-protected-by-备份计划 • rds-resources-protected-by-备份计划	2021 年 8 月 20 日
Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包： • NZISM 操作最佳实践	2021 年 8 月 20 日

安全 Amazon SNS 策略更新	在本版本中， Amazon Config 更新了使用服务相关角色时的 Amazon SNS 主题的 IAM 政策声明，以便在主题策略`sourceARN` and/or `sourceAccountId` 中加入限制访问的安全保护。这有助于确保 Amazon SNS 仅代表预期用户和场景访问您的资源。 将更新以下页面： • Amazon SNS 主题的权限	2021 年 8 月 17 日
安全 Amazon Lambda 政策更新	在此版本中， Amazon Config 更新了 Amazon Config 自定义规则的 Amazon Lambda 基于资源的策略，使其在调用请求`sourceARN` and/or `sourceAccountId` 中包含限制访问权限的安全保护。这有助于确保 Amazon Lambda 仅代表预期的用户和场景访问您的资源。 将更新以下页面： • AWS::Config::ConfigRule • 为以下对象开发自定义规则 Amazon Config	2021 年 8 月 12 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon Kinesis 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 8 月 6 日

Amazon Config 支持新的一致性包	在此版本中， Amazon Config 支持以下一致性包： • Esquema Nacional de Seguridad（ ENS ）High 操作最佳实践 将更新以下合规包： • Well-Architecte Amazon d 框架可靠性支柱的运营最佳实践 • Well-Architecte Amazon d Framework 安全支柱的运营最佳实践 • Esquema Nacional de Seguridad（ ENS ）Low 操作最佳实践 • Esquema Nacional de Seguridad（ ENS ）Medium 操作最佳实践 • HIPAA 安全操作最佳实践	2021 年 7 月 30 日
Amazon Config 自定义规则的示例 Amazon Lambda 函数	在此版本中，在Amazon Config 规则示例函数 (Python) 中 Amazon Config 提供了 Python 示例 Amazon Lambda 函数。	2021 年 7 月 29 日

安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略和 `AWS_ConfigRole` 策略现在授予列出日志组的标签，列出状态机的标签，以及列出所有状态机的权限。这些策略现在授予获取有关状态机的详细信息的权限。这些政策现在还支持对亚马逊 EC2 系统管理器 (SSM)、亚马逊弹性容器注册表、亚马逊、亚马逊数据 Firehose FSx、亚马逊管理流媒体 Kafka（亚马逊 MSK）、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Route 53、亚马逊 AI SageMaker 、亚马逊简单通知服务、和的额外权限。 Amazon Database Migration Service Amazon Global Accelerator Amazon Storage Gateway有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2021 年 7 月 28 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录 Amazon Backup 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 7 月 14 日

Amazon Config 支持新的一致性包	在此版本中，Amazon Config 支持以下一致性包： • CIS 关键安全控制操作最佳实践 v8 IG1 • CIS 关键安全控制操作最佳实践 v8 IG2 • CIS 关键安全控制操作最佳实践 v8 IG3 • NIST 1800 25 操作最佳实践	2021 年 7 月 9 日
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • ssm-document-not-public • s3--account-level-public-access 区块-周期性	2021 年 6 月 25 日
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • ec2-instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip 已禁用	2021 年 6 月 10 日

安全 IAM 更新	现在，该AWSConfig ServiceRolePolicy 策略和AWS_ConfigRole 策略授予查看有关 IAM Access Analyzer 的 Amazon Systems Manager 文档和信息的权限。这些策略现在支持亚马逊 Kinesis、亚马逊、亚马逊 EMR、 ElastiCache亚马逊 Route 53 和 Amazon Network Firewall亚马逊关系数据库服务 (Amazon RDS) 的其他 Amazon 资源类型。这些权限更改 Amazon Config 允许调用支持这些资源类型 APIs 所需的只读权限。这些策略现在还支持筛选lambda-inside-vpc Amazon Config 托管规则的 Lambda @Edge 函数。有关更多信息，请参阅适用于 Amazon Config的Amazon 托管策略。	2021 年 6 月 8 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-已启用 • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	2021 年 5 月 19 日

Amazon Config 支持新的资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon Elastic File System 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 5 月 13 日
安全 IAM 更新	现在，该AWSConfig ServiceRolePolicy 策略和AWS_ConfigRole 策略授予允许 Amazon Config 对 API Gateway 进行只读 GET 调用的权限，以支持 API Gateway 的配置规则。这些策略还增加了允许 Amazon Config 以 APIs只读方式调用 Amazon Simple Storage Service (Amazon S3) 的权限，这些权限是支持AWS::S3::AccessPoint 新资源类型所必需的。有关更多信息，请参阅适用于 Amazon Config的 Amazon 托管策略。	2021 年 5 月 10 日
Amazon Config 自定义规则	将更新开发人员指南中的以下页面： • 自定义规则入门 Amazon Config • 为以下对象开发自定义规则 Amazon Config	2021 年 4 月 30 日

Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • aurora-mysql-backtracking-enabled • ec2-instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-已启用升级 • redshift-enhanced-vpc-routing-已启用	2021 年 4 月 15 日

安全 IAM 更新	现在，该AWSConfigServiceRolePolicy AWS_ConfigRole 策略和策略授予查看有关 Amazon Systems Manager 指定文档的信息的权限。这些政策现在还支持亚马逊弹性文件系统 Amazon Backup、亚马逊、亚马逊简单存储服务 (Amazon S3) ElastiCache、亚马逊弹性计算云 (亚马逊)、亚马逊 Kinesis、 EC2亚马逊 AI 和 SageMaker 亚马逊 Route 53 的其他 Amazon 资源类型。Amazon Database Migration Service这些权限更改 Amazon Config 允许调用支持这些资源类型 APIs 所需的只读权限。有关更多信息，请参阅适用于Amazon Config的Amazon 托管策略。	2021 年 4 月 14 日

将一致性包合规性作为配置项目 () CIs	在此版本中，Amazon Config 支持将一致性包合规性作为配置项目。这使您能够： • 查看合规包的合规状态的变更时间线 • 汇总合规包跨多个账户和区域的合规性 • 使用高级查询来检查合规包的合规性 将更新以下数据类型： • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary 将更新开发人员指南中的以下页面： • 在“合规包”控制面板中查看合规性数据 • 查看合规包的合规性历史记录时间线 • 在聚合器控制面板中查看合规性数据 • 查询 Amazon 资源的当前配置状态 • 支持的资源类型	2021 年 3 月 30 日

分页更新	在此版本中， Amazon Config 高级查询功能现在支持对包含聚合函数（例如 COUNT 和 SUM）的查询进行分页。您现在可以使用高级查询通过分页获取聚合查询的完整结果，分页以前限制为 500 行。有关更多信息，请参阅查询 Amazon 资源的当前配置状态	2021 年 3 月 26 日
区域支持	在此版本中 Amazon Config ，亚太地区（大阪）地区现在支持 Amazon Config 规则。	2021 年 3 月 4 日
Amazon Config 支持新的资源类型	在此版本中，您可以使用记录 Amazon Config 对亚马逊弹性容器注册表、亚马逊弹性容器服务和亚马逊弹性 Kubernetes Service 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 2 月 25 日

KMS 加密支持	在此版本中，Amazon Config 允许您对由 S3 存储桶交付的对象使用基于 KMS Amazon Config 的加密。 将更新以下数据类型： • DeliveryChannel • PutDeliveryChannel 将更新开发人员指南中的以下页面： • KMS 密钥的权限 • 分配给的 IAM 角色的权限 Amazon Config	2021 年 2 月 16 日
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	2021 年 2 月 16 日
已保存的查询区域支持	在此版本中，Amazon GovCloud（美国东部）和 Amazon GovCloud（美国西部）地区现在支持保存的查询。	2021 年 2 月 15 日
高级查询区域支持	在此版本中，现已在非洲（开普敦）和欧洲地区（米兰）区域支持高级查询。有关更多信息，请参阅查询 Amazon 资源的当前配置状态。	2021 年 2 月 15 日

Amazon Config 可通过 RSS 提要获取文档历史记录通知	现在，您可以通过订阅 RSS 提要来接收有关 Amazon Config 文档更新的通知。	2021 年 1 月 1 日

早期更新

下表描述了 2020 年 12 月 31 日 Amazon Config 之前的文档发布历史。

更改	描述	发行日期
已保存的查询支持	在此版本中， Amazon Config 允许您保存查询。保存查询后，您可以对其进行搜索，将其复制到查询编辑器，以及对其进行编辑或将其删除。有关如何保存查询的更多信息，请参阅使用适用于 Amazon Config 的 SQL 查询编辑器进行查询（控制台）和使用适用于 Amazon Config 的 SQL 查询编辑器进行查询（Amazon CLI）。 有关的更多信息 APIs，请参阅 Amazon Config API 参考： • PutStoredQuery • GetStoredQuery • ListStoredQueries • DeleteStoredQuery 另请参阅 Amazon Config 的服务限制	2020 年 12 月 21 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • api-gw-ssl-enabled • api-gw-xray-enabled	2020 年 12 月 17 日

更改	描述	发行日期
	• beanstalk-enhanced-health-reporting-已启用 • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-已启用 • rds-cluster-iam-authentication-已启用 • redshift-cluster-kms-enabled • s3-bucket-level-public-access-禁止使用 • subnet-auto-assign-public-ip 已禁用 • vpc-network-acl-unused-检查	
Amazon Config 支持 Amazon Network Firewall	在此版本中，您可以使用记录 Amazon Config 对 Amazon Network Firewall FirewallPolicy RuleGroup、和防火墙资源类型的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2020 年 12 月 4 日
文档更新	Amazon Config 添加了对委派管理员帐户中组织范围的资源数据聚合的支持。您现在可以使用委派管理员账户聚合 Amazon Organizations 中所有组织成员账户中的资源配置和合规性数据。 有关更多信息，请参阅PutConfigurationAggregator、为 Amazon Config 创建聚合器和注册 Amazon Config 的委托管理员。	2020 年 12 月 4 日

更改	描述	发行日期
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • iam-customer-policy-blocked-kms 动作 • iam-inline-policy-blocked-kms 动作	2020 年 9 月 17 日
Amazon Config 支持 Amazon WAF v2	在此版本中，您可以使用记录 Amazon Config 对 Amazon WAF v2 WebACL IPSet、、 RegexPatternSet RuleGroup、 ManagedRuleSet 和资源类型的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2020 年 9 月 1 日
文档更新	完全访问权限 Amazon Config 中添加了关于创建授予完全访问权限的自定义权限的注释。 已更新有关以下规则的文档： • s3-已bucket-server-side-encryption 启用 • ??? • ec2-managedinstance-platform-check	2020 年 8 月 24 日
文档更新	更新了 ??? 和 ??? 模板。	2020 年 8 月 14 日
文档更新	添加了关系查询示例。有关更多信息，请参阅 Amazon Config 的关系查询示例	2020 年 7 月 30 日

更改	描述	发行日期
文档更新	将更新以下数据类型： • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus	2020 年 7 月 23 日
Amazon Config 支持 S Amazon ystems Manager 资源类型	在此版本中，您可以使用 Amazon Config 记录对 S Amazon ystems Manager 文件数据资源类型的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2020 年 7 月 9 日

更改	描述	发行日期
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • ??? • ??? • ??? • ??? • ??? • ??? • ??? • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-检查 • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-访问 • eks-secrets-encrypted • ??? • ??? • ??? • ??? • ??? • rds-in-backup-plan • ??? • ??? • rds-logging-enabled • redshift-backup-enabled • ???	2020 年 7 月 9 日

更改	描述	发行日期
	• wafv2-logging-enabled 有关更多信息，请参阅 Amazon Config 托管规则列表。	
多账户多区域数据聚合区域支持	在此版本中，亚太地区（香港）和中东（巴林）区域现已支持多账户多区域数据聚合。有关更多信息，请参阅Multi-Account Multi-Region Data Aggregation和Amazon Config 多账户多区域数据聚合的故障排除。	2020 年 7 月 1 日
高级查询区域支持	在此版本中，亚太地区（香港）和中东（巴林）区域现已支持高级查询。有关更多信息，请参阅 使用查询 Amazon 资源的当前配置状态 Amazon Config	2020 年 7 月 1 日
文档更新	已更新有关以下规则的文档： • ??? • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • ??? • s3-bucket-policy-grantee-check	2020 年 6 月 30 日
文档更新	文档已更新，其中包含有关安全性的信息 Amazon Config。请参阅安全性 Amazon Config。	2020 年 6 月 24 日

更改	描述	发行日期
Amazon Config 更新托管规则	在此版本中，Amazon Config 支持以下托管规则： • ??? • ??? • ec2-ebs-encryption-by-default • ??? • redshift-require-tls-ssl • ??? • s3-default-encryption-kms • securityhub-enabled • ??? 有关更多信息，请参阅 Amazon Config 托管规则列表。	2020 年 5 月 28 日

更改	描述	发行日期
委派管理员支持	在此版本中，除了管理账户之外，您还可以从组织中的任何委托成员账户部署 Amazon Config 规则和合规包。 有关的更多信息 APIs，请参阅 Amazon Config API 参考： • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRuleStatuses • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePackStatuses • GetOrganizationConformancePackDetailedStatus 有关更多信息，请参阅 Amazon Config 的服务限制。	2020 年 5 月 27 日
Amazon Config 规则区域支持	在此版本中，非洲（开普敦）和欧洲（米兰）地区支持的 Amazon Config 规则很少。有关规则及支持它们的区域的详细列表，请参阅 Amazon Config 托管规则列表	2020 年 4 月 28 日

更改	描述	发行日期
Amazon Config 支持 S Amazon ecrets Manager	在此版本中，您可以使用记录 Amazon Config 对您的 Secrets Manager 密钥的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2020 年 4 月 20 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • secretsmanager-rotation-enabled-check • ??? 有关更多信息，请参阅 Amazon Config 托管规则列表。	2020 年 4 月 16 日
文档更新	Amazon Config 本开发者指南中提供了限制。有关更多信息，请参阅 Amazon Config 的服务限制。	2020 年 4 月 8 日
文档更新	通过 Amazon CloudFormation 注册表管理（即created/updated/deleted）的第三方资源会自动 Amazon Config 作为配置项目进行跟踪。有关更多信息，请参阅 使用 Amazon CLI 记录 Amazon Config 第三方资源的配置。	2020 年 3 月 30 日
文档更新	Amazon Config 托管规则已更新以包含 Amazon Web Services 区域 信息。有关更多信息，请参阅 Amazon Config 托管规则列表。	2020 年 3 月 27 日

更改	描述	发行日期
Amazon Config 支持 Amazon SNS 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon SNS 主题的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2020 年 3 月 6 日
多账户多区域数据聚合区域支持	在此版本中，多账户多区域数据聚合现在在欧洲（斯德哥尔摩）区域中受支持。有关更多信息，请参阅 Multi-Account Multi-Region Data Aggregation	2020 年 3 月 5 日
高级查询区域支持	在此版本中，欧洲（斯德哥尔摩）区域现在支持高级查询。有关更多信息，请参阅 使用查询 Amazon 资源的当前配置状态 Amazon Config	2020 年 3 月 5 日
Amazon Config 允许您使用配置聚合器运行高级查询	在此版本中， Amazon Config 增加了对使用配置聚合器基于资源配置属性运行高级查询的支持，使您能够在多个账户和区域中运行相同的查询。有关更多信息，请参阅 使用查询 Amazon 资源的当前配置状态 Amazon Config。 在此版本中， Amazon Config 添加了 `SelectAggregateResourceConfig` API。有关更多信息，请参阅 Amazon Config API 参考SelectAggregateResourceConfig中的：	2020 年 2 月 28 日

更改	描述	发行日期
Amazon Config 支持 Amazon SQS 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon SQS 队列的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2020 年 2 月 13 日
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • api-gw-execution-logging-已启用 • ec2-stopped-instance • elasticache-redis-cluster-automatic-备份检查 • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • ??? • sagemaker-endpoint-configuration-kms-密钥已配置 • service-vpc-endpoint-enabled 有关更多信息，请参阅 Amazon Config 托管规则列表。	2019 年 12 月 20 日

更改	描述	发行日期
记录自定义资源类型的配置	在此版本中， Amazon Config 引入了对自定义资源类型记录配置的支持。您可以使用 Amazon Config 控制台和将第三方资源的配置数据发布到 Amazon Config 并查看和监控资源清单和配置历史记录 APIs。有关更多信息，请参阅 使用 Amazon CLI 记录 Amazon Config 第三方资源的配置。 有关的更多信息 APIs，请参阅 Amazon Config API 参考： • DeleteResourceConfig • PutResourceConfig	2019 年 11 月 20 日
Amazon Config 支持 Amazon OpenSearch 服务和 Amazon Key Managemen t Service 资源类型	在此版本中，您可以使用记录 Amazon Config 对您的 Amazon S OpenSearch ervice 域和 Amazon Key Management Service 密钥的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2019 年 11 月 11 日

更改	描述	发行日期
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • dms-replication-not-public • emr-kerberos-enabled • ??? • kms-cmk-not-scheduled-用于删除 • sagemaker-notebook-no-direct-互联网接入 • sagemaker-notebook-instance-kms-密钥已配置 • ??? 有关更多信息，请参阅 Amazon Config 托管规则列表。	2019 年 10 月 10 日
Amazon Config 支持 Amazon RDS 资源类型	在此版本中，您可以使用记录 Amazon Config 对亚马逊关系数据库服务 (Amazon RDS) DBCluster 和 DBCluster快照的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2019 年 9 月 17 日
Amazon Config 支持 Amazon QLDB 资源类型	在此版本中，您可以使用记录 Amazon Config 对亚马逊量子账本数据库 (QLDB) 账本资源类型的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2019 年 9 月 10 日

更改	描述	发行日期
Amazon Config 允许您根据规则对不合规的资源进行 Amazon Config 自动修复	在本版本中，根据 Amazon Config 规则的评估， Amazon Config 引入了使用 Amazon Systems Manager 自动化文档对不合规资源应用自动补救的支持。有关更多信息，请参阅 使用修复不合规的资源 Amazon Config。 在此版本中， Amazon Config 添加了以下新内容 APIs。有关更多信息，请参阅 Amazon Config API 参考： • PutRemediationExceptions • DescribeRemediationExceptions • DeleteRemediationExceptions	2019 年 9 月 5 日

更改	描述	发行日期
Amazon Config 更新托管规则	在此版本中， Amazon Config 支持以下托管规则： • alb-http-to-https-重定向检查 • ??? • ??? • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-检查 • ??? • ??? • ??? • ??? • ??? • ??? 有关更多信息，请参阅 Amazon Config 托管规则列表。	2019 年 8 月 22 日

更改	描述	发行日期
Amazon Config 更新托管规则	在此版本中， Amazon Config 更新了以下托管规则： • ??? • ??? • ec2-security-group-attached-to-eni • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • ??? • vpc-sg-open-only-to-authorized-ports 有关更多信息，请参阅 Amazon Config 托管规则列表。	2019 年 7 月 31 日
Amazon Config 支持 Amazon EC2 资源类型	在此版本中，您可以使用记录 Amazon Config 对以下 Amazon EC2 资源 VPCEndpoint、 VPCEndpoint服务和 VPCPeering连接的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2019 年 7 月 12 日
Amazon Config 支持 Amazon S3 和亚马逊 EC2 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon S3 AccountPublicAccessBlock 资源和以下 Amazon EC2 资源的配置更改； NatGateway EgressOnlyInternetGateway、和 FlowLog。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2019 年 5 月 17 日

更改	描述	发行日期
Amazon Config 更新托管规则	在此版本中， Amazon Config 更新了以下托管规则： • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited 有关更多信息，请参阅 Amazon Config 托管规则列表。	2019 年 5 月 7 日
Amazon Config 允许您使用删除修复操作 Amazon Web Services 管理控制台。	在此版本中， Amazon Config 引入了对使用删除修复操作的支持 Amazon Web Services 管理控制台。有关更多信息，请参阅 使用修复不合规的资源 Amazon Config。	2019 年 4 月 24 日
Amazon Config 支持新的托管规则	此版本支持新的托管规则：???。 有关更多信息，请参阅 Amazon Config 托管规则列表	2019 年 4 月 7 日
Amazon Config 支持 Amazon API Gateway 资源类型	在此版本中，您可以使用记录 Amazon Config 对以下 Amazon API Gateway 资源的配置更改：Api (API)、(REST WebSocket API)、阶段 RestApi （ API 阶段 ）和阶段（ REST WebSocket API 阶段 ）和阶段（ REST API 阶段 ）。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2019 年 3 月 20 日

更改	描述	发行日期
Amazon Config 允许你运行高级查询	在此版本中， Amazon Config 增加了对基于资源配置属性运行高级查询的支持。有关更多信息，请参阅 使用查询 Amazon 资源的当前配置状态 Amazon Config。 在此版本中， Amazon Config 添加了 `SelectResourceConfig` API。有关更多信息，请参阅 Amazon Config API 参考SelectResourceConfig中的：	2019 年 3 月 19 日
Amazon Config 允许您为 Amazon Config 资源分配标签	在此版本中， Amazon Config 引入了对三种 Amazon Config 资源的基于标签的访问控制的支持 — `ConfigRule`, `ConfigurationAggregator`, 和`AggregationAuthorization` 。有关更多信息，请参阅 标记您的 Amazon Config 资源。 在此版本中，您可以使用以下数据类型添加、删除或列出您的 Amazon Config 资源中的标签。有关更多信息，请参阅 Amazon Config API 参考： • ListTagsForResource • TagResource • UntagResource	2019 年 3 月 14 日

更改	描述	发行日期
Amazon Config 允许您根据规则对不合规的资源进行 Amazon Config 修复	在此版本中， Amazon Config 引入了使用 Amazon Systems Manager 自动化文档对不合规资源进行补救的支持，这些资源由 Amazon Config Rules 评估。有关更多信息，请参阅 使用修复不合规的资源 Amazon Config。 在此版本中， Amazon Config 添加了以下新内容 APIs。有关更多信息，请参阅 Amazon Config API 参考： • DeleteRemediationConfiguration • DescribeRemediationConfigurations • DescribeRemediationExecutionStatus • PutRemediationConfigurations • StartRemediationExecution	2019 年 3 月 12 日

更改	描述	发行日期
Amazon Config 支持中国（宁夏）区域的 Amazon Config 规则	此版本仅支持中国（宁夏）区域的 54 Amazon Config 条规则。有关更多信息，请参阅 Amazon Config 托管规则列表。 但是，目前 Amazon Config 不支持中国（宁夏）区域的以下规则： • acm-certificate-expiration-check • cmk-backing-key-rotation-已启用 • cloudformation-stack-drift-detection-检查 • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-已启用验证 • codebuild-project-envvar-awscred-检查 • codebuild-project-source-repo-url-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-enabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-检查 • fms-webacl-rulegroup-association-检查 • guardduty-enabled-centralized	2019 年 3 月 12 日

更改	描述	发行日期
	• lambda-function-public-access-禁止 • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa 已启用 • root-account-mfa-enabled • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-grantee-check • s3-bucket-policy-not-more-宽容 • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited • s3-已bucket-server-side-encryption启用 • s3-bucket-ssl-requests-only	
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • iam-user-mfa-enabled 有关更多信息，请参阅 Amazon Config 托管规则列表	2019 年 1 月 21 日
Amazon Config 支持 Service Catalog 资源类型	在此版本中，您可以使用记录 Amazon Config 对以下 Service Catalog 资源的配置更改：CloudFromation 产品、预配置产品和产品组合。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2019 年 1 月 11 日

更改	描述	发行日期
服务关联 Amazon Config 规则支持	在此版本中，Amazon Config 添加了一个新的托管配置规则，该规则支持其他 Amazon 服务在您的账户中创建 Amazon Config 规则。有关更多信息，请参阅 服务相关的 Amazon Config 规则。	2018 年 11 月 20 日
Amazon Config 允许您聚合 Amazon 资源的配置数据	在此版本中，Amazon Config 引入了对聚合 Amazon 资源配置数据的支持。有关更多信息，请参阅 在 Amazon Config 聚合器控制面板中查看合规性和清单数据。 在此版本中，Amazon Config 添加了以下新内容 APIs。有关更多信息，请参阅 Amazon Config API 参考： • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResourceCounts • GetAggregateResourceConfig • ListAggregateDiscoveredResources	2018 年 11 月 19 日
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • cloudformation-stack-drift-detection-检查 • ??? • ??? 有关更多信息，请参阅 Amazon Config 托管规则列表	2018 年 11 月 19 日

更改	描述	发行日期
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • access-keys-rotated • cloud-trail-cloud-watch-启用日志 • cloud-trail-encryption-enabled • cloud-trail-log-file-已启用验证 • cmk-backing-key-rotation-已启用 • iam-policy-no-statements-with-admin-access • ??? • iam-root-access-key-检查 • iam-user-unused-credentials-检查 • mfa-enabled-for-iam-控制台访问权限 • multi-region-cloudtrail-enabled • ??? • vpc-flow-logs-enabled 有关更多信息，请参阅 Amazon Config 托管规则列表	2018 年 11 月 12 日
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • ??? • ??? • ??? • ??? 有关更多信息，请参阅 Amazon Config 托管规则列表	2018 年 10 月 24 日

更改	描述	发行日期
合规性历史记录支持	在此版本中， Amazon Config 现在支持存储 Amazon Config 规则评估的资源的合规性历史记录。有关更多信息，请参阅 查看资源和规则的合规性历史记录时间线。	2018 年 10 月 18 日
多账户多区域数据聚合区域支持	在此版本中，多账户多区域数据聚合现在可在六个新区域中受支持。有关更多信息，请参阅 Multi-Account Multi-Region Data Aggregation	2018 年 10 月 4 日
Amazon Config 支持规则操作的资源级权限 Amazon Config APIs	在此版本中， Amazon Config 支持某些 Amazon Config 规则 API 操作的资源级权限。有关支持的更多信息 APIs，请参阅Amazon Config 规则 API 操作支持的资源级权限。	2018 年 10 月 1 日
Amazon Config 支持 CodePipeline 资源类型	在此版本中 Amazon Config ，您可以使用记录 Amazon CodePipeline 资源类型的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2018 年 9 月 12 日

更改	描述	发行日期
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • ec2-管理instance-managed-by-systems器 • ??? • ec2-managedinstance-patch-compliance-status-check • guardduty-enabled-centralized • ??? • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-not-more-宽容 有关更多信息，请参阅 Amazon Config 托管规则列表	2018 年 9 月 5 日
Amazon Config 支持 S Amazon ystems Manager 资源类型	在此版本中，您可以使用 Amazon Config 记录对 S Amazon ystems Manager 补丁合规性和关联合规性资源类型的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2018 年 8 月 9 日
Amazon Config 允许您使用删除 Amazon Config 数据 Amazon Web Services 管理控制台	在此版本中， Amazon Config 引入了对保留期的支持 Amazon Web Services 管理控制台。在中 Amazon Web Services 管理控制台，您可以为自己的自定义数据保留期限`ConfigurationItems` 。有关更多信息，请参阅 删除 Amazon Config 数据。	2018 年 8 月 7 日

更改	描述	发行日期
Amazon Config 支持 Amazon Shield 资源类型	在此版本中，您可以使用记录 Amazon Config 对 Amazon Shield 保护资源类型的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2018 年 8 月 7 日
Amazon Config 支持 Amazon PrivateLink	在此版本中 Amazon PrivateLink，Amazon Config 支持在亚马逊虚拟私有云 (VPC) Private Cloud (VPC) 之间 Amazon Config 以及完全在网络内 Amazon 路由数据。有关更多信息，请参阅 将 Amazon Config 与接口 Amazon VPC 端点一起使用。	2018 年 7 月 31 日
Amazon Config 允许您删除 Amazon Config 数据	此版本 Amazon Config 引入了对保留期的支持。 Amazon Config 允许您通过为自己的数据指定保留期来删除数据`ConfigurationItems` 。有关更多信息，请参阅 删除 Amazon Config 数据。 在此版本中， Amazon Config 添加了以下新内容 APIs。有关更多信息，请参阅 Amazon Config API 参考： • PutRetentionConfiguration • DescribeRetentionConfigurations • DeleteRetentionConfiguration	2018 年 5 月 25 日

更改	描述	发行日期
Amazon Config 支持新的托管规则	此版本支持以下两新的托管规则： • ??? • s3-bucket-replication-enabled • iam-policy-blacklisted-check 有关更多信息，请参阅 Amazon Config 托管规则列表	2018 年 5 月 10 日
Amazon Config 支持 Amazon X-Ray 资源类型	在此版本中 Amazon Config ，您可以使用记录 Amazon X-Ray EncryptionConfig 资源类型的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2018 年 5 月 1 日
Amazon Config 支持 Amazon Lambda 资源类型和一个新的托管规则	在此版本中，您可以使用 Amazon Config 来记录对 Amazon Lambda 函数资源类型的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。 此版本还支持 ??? 托管规则。有关更多信息，请参阅 Amazon Config 托管规则	2018 年 4 月 25 日
Amazon Config 支持 Amazon Elastic Beanstalk 资源类型	在此版本中，您可以使用记录 Amazon Config 对 Amazon Elastic Beanstalk 应用程序、应用程序版本和环境资源的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2018 年 24 月 4 日

更改	描述	发行日期
Amazon Config 支持新的托管规则	此版本支持以下两新的托管规则： • fms-webacl-resource-policy-检查 • fms-webacl-rulegroup-association-检查 有关更多信息，请参阅 Amazon Config 托管规则列表	2018 年 4 月 4 日

更改	描述	发行日期
多账户多区域数据聚合	在此版本中，Amazon Config 引入了多账户多区域数据聚合。此功能允许您将来自多个账户或一个组织以及多个地区的 Amazon Config 数据聚合到一个聚合器账户中。有关更多信息，请参阅 Multi-Account Multi-Region Data Aggregation。 在此版本中，Amazon Config 添加了以下新内容 APIs。有关更多信息，请参阅 Amazon Config API 参考： • PutConfigurationAggregator • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregationAuthorization • DescribeAggregationAuthorizations • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfigRule • DescribeConfigurationAggregators • DescribeConfigurationAggregatorSourcesStatus • DeleteAggregationAuthorization • DeleteConfigurationAggregator	2018 年 4 月 4 日

更改	描述	发行日期
Amazon Config 使用 Amazon CloudWatch 事件进行监控	在此版本中，使用 Amazon CloudWatch Events 来检测 Amazon Config 事件状态的变化并做出反应。 有关更多信息，请参阅 使用 Amazon EventBridge 监控 Amazon Config。	2018 年 3 月 29 日
新的 API 操作	在此版本中， Amazon Config 增加了对 BatchGetResourceConfigAPI 的支持，允许您批量检索一个或多个资源的当前状态。	2018 年 3 月 20 日
Amazon Config 支持 Amazon WAF RuleGroup 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon WAF RuleGroup 和 Amazon WAF RuleGroup 区域资源的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2018 年 2 月 15 日

更改	描述	发行日期
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • elb-acm-certificate-required • elb-custom-security-policy-ssl-check • elb-predefined-security-policy-ssl 检查 • ??? • ??? • ??? • s3-已bucket-server-side-encryption 启用 有关更多信息，请参阅 Amazon Config 托管规则列表	2018 年 1 月 25 日
Amazon Config 支持 Elastic Load Balancing 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Elastic Load Balancing 经典负载均衡器的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2017 年 11 月 17 日

更改	描述	发行日期
Amazon Config 支持 Amazon CloudFront 和 Amazon WAF 资源类型	在此版本中，您可以使用 Amazon Config 记录 CloudFront 分发和直播分发的配置更改。 在此版本中，您可以使用记录 Amazon Config 对以下资源 Amazon WAF 和 Amazon WAF 区域资源的配置更改；基于费率的规则、规则和 Web ACL。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2017 年 11 月 15 日
Amazon Config 支持 Amazon CodeBuild 资源类型	在此版本中，您可以使用 Amazon Config 来记录 Amazon CodeBuild 项目的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2017 年 10 月 20 日
Amazon Config 支持 Auto Scaling 资源和一条新的托管规则	在此版本中，您可以使用记录 Amazon Config 以下 Auto Scaling 资源的配置更改：组、启动配置、计划操作和扩展策略。 有关更多信息，请参阅 支持的资源类型 Amazon Config。 此版本还支持以下托管规则： • ??? 有关更多信息，请参阅 Amazon Config 托管规则	2017 年 9 月 18 日

更改	描述	发行日期
Amazon Config 支持 Amazon CodeBuild 资源类型	在此版本中，您可以使用 Amazon Config 来记录 Amazon CodeBuild 项目的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	2017 年 10 月 20 日
Amazon Config 支持 Auto Scaling 资源和一条新的托管规则	在此版本中，您可以使用记录 Amazon Config 以下 Auto Scaling 资源的配置更改：组、启动配置、计划操作和扩展策略。 有关更多信息，请参阅 支持的资源类型 Amazon Config。 此版本还支持以下托管规则： • ??? 有关更多信息，请参阅 Amazon Config 托管规则	2017 年 9 月 18 日
Amazon Config 支持 DynamoDB 表资源类型和一个新的托管规则	在此版本中，您可以使用记录 Amazon Config 对您的 DynamoDB 表的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。 此版本支持以下托管规则： • dynamodb-autoscaling-enabled 有关更多信息，请参阅 Amazon Config 托管规则	2017 年 9 月 8 日

更改	描述	发行日期
Amazon Config 支持两条适用于 Amazon S3 的新托管规则	此版本支持两条新的托管规则： • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited 有关更多信息，请参阅 Amazon Config 托管规则	2017 年 8 月 14 日
Amazon Config 控制台中的新页面	您可以使用 Amazon Config 控制台中的控制面板查看以下内容： • 资源总数 • 规则总数 • 不合规资源数 • 不合规规则数 有关更多信息，请参阅 查看 Amazon Config 控制面板	2017 年 7 月 17 日
新的 API 操作	您可以使用该GetDiscoveredResourceCounts操作为您返回资源类型的数量、每种资源类型的数量以及在某个区域中记录的 Amazon Config 资源总数 Amazon Web Services 账户。	2017 年 7 月 17 日

更改	描述	发行日期
Amazon Config 支持 Amazon CloudFormation 堆栈资源类型和一个新的托管规则	在此版本中，您可以使用 Amazon Config 来记录 Amazon CloudFormation 堆栈的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。 此版本支持以下托管规则： • ??? 有关更多信息，请参阅 Amazon Config 托管规则	2017 年 6 月 7 日
新增和更新的内容	此版本增加了对加拿大（中部）地区和南美洲（圣保罗）地区 Amazon Config 规则的支持。 有关所有支持 Amazon Config 和 Config 规则的区域，请参阅中的Amazon Web Services 区域 和终端节点Amazon Web Services 一般参考。	2017 年 7 月 5 日
新增和更新的内容	Amazon Config 该 Amazon GovCloud (US) 地区提供规则。有关更多信息，请参阅 Amazon GovCloud (US) 《用户指南》。 有关支持的区域 Amazon Config，请参阅中的Amazon Web Services 区域和终端节点Amazon Web Services 一般参考。	2017 年 6 月 8 日

更改	描述	发行日期
Amazon Config 支持 Amazon CloudWatch 警报资源类型和三个新的托管规则	在此版本中，您可以使用记录 Amazon Config 对您的 Amazon CloudWatch 警报的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。 此版本支持三条新的托管规则： • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • ??? 有关更多信息，请参阅 Amazon Config 托管规则	2017 年 6 月 1 日
新增和更新的内容	此版本支持为以下托管规则指定应用程序版本号： • ec2-managedinstance-applications-blacklisted • ec2-managedinstance-applications-required 有关更多信息，请参阅 Amazon Config 托管规则	2017 年 6 月 1 日
新增和更新的内容	此版本增加了对亚太地区（孟买）地区 Amazon Config 规则的支持。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 区域 和端点。	2017 年 4 月 27 日

更改	描述	发行日期
新增和更新的内容	此版本支持更新的控制台体验，可让您首次将 Amazon Config 托管规则添加到您的账户。 首次或在新区域设置 Amazon Config 规则时，可以按名称、描述或标签搜索 Amazon 托管规则。您可以选择 Select all 以选择所有规则，或者选择 Clear all 以清除所有规则。 有关更多信息，请参阅添加、查看、更新和删除规则（控制台）。	2017 年 4 月 5 日
Amazon Config 支持新的托管规则	此版本支持以下新托管规则： • acm-certificate-expiration-check • ??? • ec2-managedinstance-inventory-blacklisted • ??? • ??? • ??? • s3-bucket-ssl-requests-only 有关更多信息，请参阅 Amazon Config 托管规则列表	2017 年 2 月 21 日
新增和更新的内容	此版本增加了对欧洲（伦敦）区域 Amazon Config 规则的支持。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 区域 和端点。	2017 年 2 月 21 日

更改	描述	发行日期
新增和更新的内容	此版本为 Amazon Config 托管规则添加了 Amazon CloudFormation 模板。您可以使用这些模板为您的账户创建托管规则。有关更多信息，请参阅 使用 Amazon Config 模板创建 Amazon CloudFormation 托管规则	2017 年 2 月 16 日
新增和更新的内容	此版本增加了对 `PutEvaluations` API 的新测试模式的支持。在自定义规则中将 `TestMode` 参数设置为 true 以验证 Amazon Lambda 函数是否将评估结果传送到。 Amazon Config不会更新现有评估，并且不会将评估结果发送到。 Amazon Config 有关更多信息，请参阅《Amazon Config API Reference》中的 PutEvaluations。	2017 年 2 月 16 日
新增和更新的内容	此版本增加了对亚太地区（首尔）和美国西部（加利福尼亚北部）区域的 Amazon Config 规则的支持。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 区域 和端点。	2016 年 12 月 21 日
新增和更新的内容	此版本增加了对 Amazon Config 欧洲（伦敦）地区的支持。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 区域 和端点。	2016 年 12 月 13 日

更改	描述	发行日期
新增和更新的内容	此版本增加了对 Amazon Config 加拿大（中部）地区的支持。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 区域 和端点。	2016 年 12 月 8 日
Amazon Config 支持 Amazon Redshift 资源类型和两个新的托管规则	在此版本中，您可以使用 Amazon Config 记录对 Amazon Redshift 集群、集群参数组、集群安全组、集群快照、集群子网组和事件订阅的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。 此版本支持两条新的托管规则： • redshift-cluster-configuration-check • redshift-cluster-maintenancesettings-check 有关更多信息，请参阅 Amazon Config 托管规则列表	2016 年 12 月 7 日
新增和更新的内容	此版本增加了对新托管规则的支持： • dynamodb-throughput-limit-check 有关更多信息，请参阅 Amazon Config 托管规则列表	2016 年 12 月 7 日

更改	描述	发行日期
新增和更新的内容	此版本增加了以下支持：可在一个账户中针对每个区域创建多达 50 条规则。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Config 限制。	2016 年 12 月 7 日
Amazon Config 支持 Amazon Sy EC2 stems Manager 的托管实例清单资源类型和三个新的托管规则	在此版本中，您可以使用 Amazon Config 记录托管实例的软件配置更改，并支持托管实例清单。 有关更多信息，请参阅 Recording Software Configuration for Managed Instances。 此版本支持三条新的托管规则： • ec2-managedinstance-inventory-blacklisted • ec2-managedinstance-applications-required • ec2-managedinstance-platform-check 有关更多信息，请参阅 Amazon Config 托管规则列表	2016 年 12 月 1 日
新增和更新的内容	Amazon Config 已在中国（北京）区域推出。	2016 年 10 月 24 日

更改	描述	发行日期
Amazon Config 支持 Amazon S3 存储桶资源和两个新的托管规则	在此版本中，您可以使用 Amazon Config 记录对 Amazon S3 存储桶的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。 此版本支持两条新的托管规则： • ??? • ??? 有关更多信息，请参阅 Amazon Config 托管规则	2016 年 10 月 18 日
新增和更新的内容	此版本增加了对美国东部（俄亥俄州）地区的支持 Amazon Config 和 Amazon Config 规则。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 区域 和端点。	2016 年 10 月 17 日

更改	描述	发行日期
新增和更新的管理规则	此更新添加了对八个新的管理规则的支持： • approved-amis-by-id • approved-amis-by-tag • ??? • desired-instance-type • ??? • iam-password-policy • ??? • ??? 您可以为以下规则指定多个参数值： • desired-instance-tenancy • required-tags 有关更多信息，请参阅 Amazon Config 托管规则列表	2016 年 10 月 4 日
Amazon Config 主机的新内容和更新内容	此更新增加了对在 Amazon Config 时间轴中查看 Amazon CloudTrail API 活动的支持。如果您的账户 CloudTrail 正在登录，则可以查看资源配置更改的创建、更新和删除 API 事件。有关更多信息，请参阅 使用 Amazon Config 查看 Amazon 资源的合规性历史记录。	2016 年 9 月 6 日

更改	描述	发行日期
Amazon Config 支持 Elastic Load Balancing 资源类型	在此版本中，您可以使用 Amazon Config 记录对 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 支持的资源类型 Amazon Config。	2016 年 8 月 31 日
新增和更新的内容	此版本增加了对亚太地区（新加坡）和亚太地区（悉尼）区域的 Amazon Config 规则的支持。有关更多信息，请参阅《Amazon Web Services 一般参考》中的 Amazon Web Services 区域 和端点。	2016 年 8 月 18 日
《Amazon Config 规则》的新内容和更新内容	此更新增加了支持，用以创建一个既可按配置更改触发、又可按您选择的定期频率触发的规则。有关更多信息，请参阅 Amazon Config 规则的组成部分 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 使用 Amazon Config 规则评估资源 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。	2016 年 7 月 25 日

更改	描述	发行日期
Amazon Config 支持 Amazon RDS 和 Amazon Certificate Manager (ACM) 资源类型	在此版本中，您可以使用 Amazon Config 记录对 Amazon Relational Database Service (Amazon RDS) 数据库实例、数据库安全组、数据库快照、数据库子网组和事件订阅的配置更改。您还可以使用记录 Amazon Config 对 ACM 提供的证书的配置更改。 有关更多信息，请参阅 支持的资源类型 Amazon Config。	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 使用配置记录器 的配置记录器。	2016 年 7 月 7 日
简化的角色创建过程和更新策略	通过此更新，简化了为创建 IAM 角色 Amazon Config 的过程。支持 Config 规则的区域中均提供了此增强功能。为支持此增强功能，使用控制台设置 Amazon Config 中的步骤、Amazon Config 传送渠道的 Amazon S3 存储桶的权限 中的示例策略及 基于身份的策略示例 Amazon Config 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	此次更新将提供更新的示例函数。	2016 年 3 月 29 日
Amazon Config 规则 GitHub 存储库	此更新将有关Amazon Config 规则 GitHub 存储库的信息添加到使用 Amazon Config 规则评估资源。此存储库为 Amazon Config 用户开发和贡献的自定义规则提供了示例函数。	2016 年 3 月 1 日

更改	描述	发行日期
Amazon Config 规则	此版本引入了 Amazon Config 规则。通过规则，您可以使用 Amazon Config 来评估您的 Amazon 资源是否符合所需的配置。有关更多信息，请参阅 使用 Amazon Config 规则评估资源。	2015 年 12 月 18 日
Amazon Config 支持 IAM 资源类型	在此版本中，您可以使用记录 Amazon Config 对您的 IAM 用户、群组、角色和客户托管策略的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2015 年 12 月 10 日
Amazon Config 支持 EC2 专用主机	在此版本中，您可以使用 Amazon Config 记录 EC2 专用主机的配置更改。有关更多信息，请参阅 支持的资源类型 Amazon Config。	2015 年 11 月 23 日
更新的权限信息	此更新添加了有关以下 Amazon 托管策略的信息 Amazon Config： • `AWS_ConfigRole` – 为 Amazon Config 授予获取有关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。 • `AWSConfigUserAccess` — 向 Amazon Config 用户授予只读访问权限。有关更多信息，请参阅 只读访问权限 Amazon Config。	2015 年 10 月 19 日

更改	描述	发行日期
Amazon Config 规则预览	此版本引入了 Amazon Config 规则预览版。通过规则，您可以使用 Amazon Config 来评估您的 Amazon 资源是否符合所需的配置。有关更多信息，请参阅 使用 Amazon Config 规则评估资源。	2015 年 10 月 7 日
新增和更新的内容	此版本增加了查找 Amazon Config 已发现资源的功能。有关更多信息，请参阅 查找 Amazon Config 发现的资源。	2015 年 8 月 27 日
新增和更新的内容	此版本增加了选择 Amazon Config 记录哪些类型资源的功能。有关更多信息，请参阅 使用 Amazon Config 记录 Amazon 资源	2015 年 6 月 23 日
新增和更新的内容	此版本添加了对以下区域的支持：亚太地区（东京）、亚太地区（新加坡）、欧洲地区（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Amazon Web Services 区域 和端点。	2015 年 4 月 6 日
新指南	此版本引入了。 Amazon Config	2014 年 11 月 12 日

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